Cybersecurity in Mexico: An In-Depth Analysis of a Fragmented Regulatory Landscape

Jersain Zadamig **Llamas Covarrubias**
https://orcid.org/0000-0003-1965-2415
Universidad de Guadalajara. México
E-mail address: jersain.llamas@academicos.udg.mx

Received: November 12th, 2024
Accepted: March 20th, 2025

DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

Abstract: Mexico's cybersecurity regulatory framework remains highly fragmented, as it comprises discrete provisions on cybercrime, national security, and data protection without forming a cohesive whole. Although progress has been made in criminal statutes and intelligence capacities, the lack of a unified cybersecurity law weakens enforcement consistency and interagency collaboration. This article offers a comprehensive analysis on existing regulatory instruments, legislative proposals from 2015 to 2025, and relevant international treaties, including the Budapest Convention and the newly adopted United Nations Convention against Cybercrime. The findings reveal persistent gaps and overlaps that hamper effective detection, mitigation, and prosecution of cyber threats, disproportionately affecting critical infrastructure and SMEs. Political disputes over surveillance powers, privacy safeguards, and alignment with global frameworks have repeatedly stalled efforts to pass integrated legislation. Further complicating the landscape, rapid technological developments such as generative artificial intelligence pose new challenges to threat detection and incident response. Nevertheless, partial alignment with international standards under the USMCA and improved global cybersecurity indices signal growing awareness of the need for more cohesive governance. The article concludes by advocating the enactment of a dedicated cybersecurity statute, separate from broader security measures, to harmonize definitions, clarify institutional mandates, and foster public-private collaboration. Enhanced interagency coordination and multi-stakeholder engagement are crucial for boosting national resilience and advancing an adaptive, rights-based approach to cybersecurity.
Keywords: cybersecurity regulation; fragmented framework; digital infrastructure; international standards.

Resumen: El marco regulatorio de ciberseguridad en México sigue caracterizándose por su fragmentación, al abarcar disposiciones dispersas en cibercrimen, seguridad nacional y protección de datos sin consolidarse en un instrumento integral.

Pese a avances en materia penal y capacidades de inteligencia, la ausencia de una ley unificada en ciberseguridad debilita la consistencia en la aplicación legal y la colaboración interinstitucional. Este artículo proporciona un análisis exhaustivo de los instrumentos normativos existentes, las propuestas legislativas entre 2015 y 2025, y los tratados internacionales pertinentes, incluido el Convenio de Budapest y la reciente Convención de las Naciones Unidas contra la Ciberdelincuencia. Los hallazgos evidencian brechas y superposiciones que obstaculizan la detección, mitigación y persecución efectiva de amenazas digitales, lo que afecta de manera desproporcionada a la infraestructura crítica y a las PYMES. Las disputas políticas en torno a facultades de vigilancia, salvaguardias de privacidad y convergencia con marcos globales han detenido reiteradamente el avance de una legislación integral. Sumado a ello, el rápido desarrollo de tecnologías como la inteligencia artificial generativa plantea nuevos desafíos para la identificación de riesgos y la respuesta a incidentes. No obstante, la alineación parcial con estándares internacionales bajo el T-MEC y mejores índices de ciberseguridad reflejan una creciente conciencia de la necesidad de mayor coherencia normativa. El artículo concluye con una propuesta para promulgar un estatuto dedicado exclusivamente a la ciberseguridad, independiente de otras disposiciones de seguridad, que armonice definiciones, clarifique mandatos institucionales y fomente la colaboración público-privada. La coordinación interinstitucional y el involucramiento de múltiples actores resultan esenciales para fortalecer la resiliencia nacional y adoptar un enfoque adaptativo y centrado en derechos humanos en materia de ciberseguridad.
Palabras clave: regulación de ciberseguridad; marco fragmentado; infraestructura digital; estándares internacionales.

Summary: I. *Introduction*. II. *Methodology*. III. *Literature Review*. IV. *Problem and Possible Solutions.* V. *Historical Context and Legislative Evolution of Cybersecurity Initiatives in Mexico*. VI. *Comprehensive Overview of Cybersecurity Provisions in Mexican Legislation.* VII. *Relevant International Cybersecurity Treaties Involving Mexico: Ratified and Pending.* VIII. *Results and Discussion*. IX. *Limitations and Future Research*. X. *Conclusions*. XI. *References*.

I. Introduction

Cybersecurity has emerged as a critical global challenge amid escalating geopolitical tensions and the rapid evolution of disruptive technologies, most notably, generative artificial intelligence. This article analyzes Mexico's current cybersecurity regulatory framework, identifying specific gaps, challenges, and the need for policy cohesion, for which it will examine both the contextual situation of world`s main reforms and the local history of legislative actions.

The 2025 Global Cybersecurity Outlook by the World Economic Forum reveals that the cyber threat landscape has become even more complex, widening the cyber resilience gap between large, resource-rich organizations and smaller enterprises, particularly in emerging econo-

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

mies like Mexico.[1] SMEs (small and medium-sized enterprises) continue to struggle with financial constraints, skill shortages, and the burdens of an increasingly fragmented regulatory environment, underscoring the urgent need for coordinated, proactive cybersecurity strategies.

Critical digital infrastructure remains highly vulnerable in Mexico, as in other Latin American countries. Cisco's Cybersecurity Readiness Index reveals that only 2% of Mexican organizations have reached a mature cybersecurity readiness level, with the majority still in formative or beginner stages. This low preparedness is worrying, as nearly 73% of companies anticipate a significant cyber incident within the next two years.[2]

The Global Cybersecurity Index (GCI) provides greater insight into Mexico's progress. In the 2020 report by the International Telecommunication Union (ITU), Mexico ranked 52nd with a score of 81.68, showing particular strengths in legal and technical measurements.[3] By 2024, Mexico had advanced to Tier 2 (Advancing) with an overall score of 85.77, indicating improvements in legal and organizational measurements.[4] However, cooperation measurements saw a slight decline, highlighting an ongoing challenge for Mexico in terms of regional and international partnerships.

Moreover, the Cost of a Data Breach Report 2024 from IBM shows that the global average cost of a data breach has risen by 10% over the past year, reaching $4.88 million. Mexican organizations are not immune to these rising costs, as many companies experience prolonged disruptions and financial losses after breaches. The report also notes that companies implementing AI and automated solutions tend to incur lower breach costs, underscoring the need for Mexico to adopt such technologies amid a widening cybersecurity skills gap.[5]

This challenge is further illustrated in the 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean, which points out that while some progress has been made, regulatory fragmentation persists in Mexico and its neighboring countries,

---

[1] World Economic Forum, *Global Cybersecurity Outlook 2025*, at 4, 16, 25 (2025).

[2] Cisco, *2024 Cybersecurity Readiness Index - Mexico,* at 2-3 (2024).

[3] International Telecommunication Union, *Global Cybersecurity Index 2020*, at 6, https://itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (last visited Nov. 11, 2024).

[4] International Telecommunication Union, *Global Cybersecurity Index 2024*, at 6, 24-25, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (last visited Nov. 11, 2024).

[5] IBM & Ponemon Institute, *Cost of a Data Breach Report 2024*, at 3-4 (2024).

leaving them more susceptible to cyber threats.[6] According to Google Cloud's Cybersecurity Forecast 2024, in order to enhance phishing and misinformation campaigns, attackers increasingly use generative AI tools, posing new challenges in distinguishing between legitimate and malicious content.[7]

According to Digital Trust Insights 2025 (Mexico edition), although 83% of organizations plan to increase their cybersecurity budgets, only 42% have identified critical business processes and 37% have developed recovery manuals. Additionally, 50% remain uncertain about risk quantification, 41% intend to deploy generative AI for threat detection and response, and 68% view cybersecurity as a competitive growth advantage. These findings highlight significant gaps in achieving effective cyber resilience despite rising investments.[8] Similarly, Accenture's Cyber-Resilient CEO Report reveals that most CEOs recognize the critical importance of cybersecurity but feel unprepared to handle emerging risks, indicating a need for stronger leadership focus and integration of cybersecurity strategies.[9]

Moreover, the 2025 Global Risks Report by the World Economic Forum points out that technology's role in geopolitical tensions is a key concern, with cyber espionage and warfare ranking fifth in the two-year outlook.[10] This high ranking reveals the growing risk that advanced cyber capabilities can be exploited to destabilize global relations and compromise critical digital infrastructure, highlighting the pressing need for robust cybersecurity measures. The IBM X-Force Threat Intelligence Index supports this view, noting an increase in identity-based cyberattacks, which are challenging defenders to detect due to the complexity of distinguishing legitimate from unauthorized user access.[11]

Finally, research by the Asociación del Internet de México and the Consejo de Datos y Tecnologías Emergentes examines digital security practices across various sectors, emphasizing the importance of public awareness and education in cybersecurity. The study suggests a significant need for improved knowledge and digital practices among the Mex-

---

[6] Inter-American Development Bank, *2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean*, at 5, 12-13 (2020).

[7] Google Cloud, *Cybersecurity Forecast 2024*, at 3-4, 8 (2024).

[8] PwC, *Digital Trust Insights 2025 - Mexico Edition* (2025).

[9] Accenture, *The Cyber-Resilient CEO*, at 4-5, 18 (2024).

[10] World Economic Forum, *Global Risks Report 2025*, at 8, 12 (2025).

[11] IBM, *X-Force Threat Intelligence Index 2024*, at 3-4, 6 (2024).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

ican public in response to the growing risks within the country's digital ecosystem.[12]

This global cybersecurity context poses an urgent challenge for Mexico. Unlike many nations that have established dedicated cybersecurity laws, Mexico's regulatory approach is fragmented across various legislative frameworks without a singular, cohesive cybersecurity law. This regulatory gap leaves Mexico's critical infrastructure, SMEs, and the broader digital ecosystem vulnerable to cyber threats. The need for an integrated cybersecurity framework is particularly compelling in light of the increase in cyber risks and the growing reliance on digital technologies in every sector of Mexican society.

This article aims to critically analyze Mexico's current cybersecurity regulatory framework, identifying specific gaps, challenges, and the need for policy cohesion. It examines Mexico's fragmented legislative approach to cybersecurity, focusing on how these legal structures address, or fall short in addressing, contemporary cyber threats. Ultimately, this article advocates in favor of strategic recommendations aimed at consolidating Mexico's regulatory landscape, encouraging international alignment, and fostering a more resilient digital infrastructure.

While there are various instruments that, although not strictly regulatory, possess binding authority due to their nature as formally administrative but materially legislative acts, this article will not address those issued by public administration. Instead, it will focus exclusively on regulations issued by representative bodies, such as the Mexican Congress and Senate. However, it is worth noting that Mexico addresses cybersecurity through several key documents. The National Cybersecurity Strategy 2017,[13] for example, is a foundational framework that outlines national cybersecurity policies and serves as a primary reference in this article. Additional instruments, including the National Development Plan, the National Public Security Program, the Sectoral Program for Security and Citizen Protection, the National Digital Strategy, and several administrative agreements, also contain relevant cybersecurity provisions.[14] This list is not exhaustive, since numerous administrative guidelines in Mexico address various aspects of cybersecurity across the public sector.

---

[12] Asociación del Internet de México & Consejo de Datos y Tecnologías Emergentes, *3er Estudio de Ciberseguridad en México 2023*, at 3-4, 6 (2023).

[13] Presidencia de la República [Office of the President], Estrategia Nacional de Ciberseguridad [National Cybersecurity Strategy] (2017) (Mex.).

[14] Inter-American Development Bank, *2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean*, at 126-129 (2020).

This research is grounded on a thorough review of legislative initiatives, regulatory provisions, and policy measures specific to cybersecurity in Mexico. First, the article presents a historical context and legislative evolution of cybersecurity initiatives in Mexico, capturing both achievements and ongoing challenges. It then provides a comprehensive overview of cybersecurity provisions within Mexican legislation, examining key areas such as cybercrime, critical infrastructure protection, and data privacy. Additionally, it explores Mexico's involvement in relevant international cybersecurity treaties, analyzing both ratified and pending agreements that shape Mexico's approach to cross-border cyber threats. Finally, the article concludes with reflections on the current state of Mexico's cybersecurity landscape and the potential pathways toward a more cohesive regulatory framework.

In light of these pressing concerns, this article explores the regulatory landscape of cybersecurity in Mexico, emphasizing the gaps, overlaps, and underlying political dynamics that have thus far impeded the formulation of a coherent, unified legal framework. By situating Mexico's experience within broader global cybersecurity challenges, the analysis highlights the interplay of legislative inertia, emerging technological threats, and the critical importance of aligning domestic policies with international conventions. The sections that follow offer a structured investigation: first, a historical contextualization of Mexico's cybersecurity initiatives, tracing the evolution of proposals and amendments; next, a comprehensive overview of existing laws that capture scattered cybersecurity provisions; and, subsequently, a review of relevant international treaties that underscore Mexico's potential pathways toward harmonization and cross-border collaboration.

The article then presents findings on how this fragmented framework impedes both public and private sector resilience, followed by a discussion that examines the legal, institutional, and societal ramifications. The concluding sections synthesize the insights gleaned from this inquiry, proposing strategic recommendations for legislative consolidation and enhanced stakeholder engagement. By mapping out the challenges and opportunities, this article aims to bolster not only Mexico's cybersecurity posture but also its readiness to adapt to rapidly evolving digital threats, an imperative that resonates well beyond national borders.

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

II. Methodology

This study adopts a mixed qualitative approach designed to capture both the doctrinal underpinnings of Mexico's cybersecurity legislation and the broader policy context in which it unfolds. Methodologically, the research proceeded in four main stages:

1. Documentary and Legislative Review:
The core of this investigation consisted of an extensive analysis of primary legal sources. This included reviewing the full texts of relevant laws, proposed bills, and amendments in the Mexican legislative record from 2015 to 2025. Legislative proposals were identified through official parliamentary documents, publicly accessible archives of the Mexican Congress and Senate, as well as official communications and press releases outlining the scope of each initiative. Particular attention was paid to the chronological evolution of these proposals, enabling a comparative assessment of how lawmakers have conceptualized cybersecurity over time and how legislative intent has shifted, or remained static, across different political administrations.

2. Doctrinal Legal Analysis:
To interpret the fragmented body of statutes and legislative drafts, a doctrinal (black-letter law) approach was employed. This method entailed a close reading of statutory language to identify explicit cybersecurity provisions, definitions, penalties, and enforcement mechanisms. By evaluating the precision of the terms (e.g., "cybercrime," "information security," "critical infrastructure," "cyber intelligence") and mapping them against broader legal frameworks (e.g., criminal, national security, and data protection laws), the study elucidates both overlaps and lacunae in the regulatory landscape. This doctrinal lens was also instrumental in distinguishing cybersecurity-specific provisions from those primarily geared toward criminal justice or intelligence gathering.

3. Comparative and Contextual Framework:
After establishing a foundation through legislative texts, the study integrated a comparative perspective using international instruments and standards. Particular focus was placed on the Budapest Convention, the newly adopted United Nations Convention against Cybercrime, and relevant clauses in the USMCA (T-MEC). By juxtaposing

Mexico's legal texts with these global norms, the research highlights the degree of alignment, potential areas of conflict, and prospects for harmonization. Concurrently, authoritative reports and indices, such as the Global Cybersecurity Index, IBM's Cost of a Data Breach Report, and the World Economic Forum's Global Cybersecurity Outlook, provided broader context on how legislative fragmentation intersects with on-the-ground cybersecurity readiness.

4. Iterative Thematic Synthesis:
Finally, an iterative thematic analysis was conducted to integrate findings from the legislative review, doctrinal interpretation, and international comparisons. Key themes, such as the conflation of cybersecurity with cybercrime, the interplay of national security concerns, and the political impediments to passing a unified cybersecurity statute, were identified, refined, and cross-referenced. This approach allowed the research to move beyond enumerating statutory gaps and, instead, discuss how institutional, political, and international factors converge to shape cybersecurity regulation in Mexico. The synthesis informed not only the problem definition and discussion sections but also the policy-oriented solutions proposed toward a more cohesive regulatory framework.

By combining rigorous legal analysis with contextual insights from international standards and sectoral reports, this methodology ensures a multifaceted understanding of Mexico's cybersecurity environment. It captures both the doctrinal intricacies of evolving legislative texts and the real-world challenges, technical, political, and organizational, that influence the feasibility and effectiveness of any proposed reforms.

II. Literature Review

Scholarly discourse on the issue of cybersecurity in Mexico has predominantly revolved around the inadequacies of its legal frameworks and the pressing need for a cohesive regulatory landscape. We will briefly describe the main branches of it as it will help us in the global comprehension of the precedent academic studies.

The early work by Diaz Gomez highlights the necessity of intersectoral collaboration, encompassing governmental, private, and civil enti-

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

ties, to effectively combat cybercrime.[15] By situating the national legal framework in a comparative international context, including potential alignment with the Budapest Convention, he underscores that safeguarding individual liberties must remain central, even as legislative initiatives increasingly prioritize security concerns. His work reveals a delicate balancing act between protecting citizens in cyberspace and preserving constitutional rights, a tension that resonates with ongoing debates over surveillance powers, data protection, and freedom of expression. Building upon these foundational insights, Piña Libien presents a hermeneutic and conceptual investigation into the interplay of cybersecurity measures and fundamental rights in Mexico's evolving information society.[16]

Standing from a geopolitical perspective, Aguilar-Antonio contends that cyberspace has evolved into a principal arena of national defense, necessitating a reconfiguration of security policies in Mexico.[17] Drawing comparisons with global cybersecurity benchmarks, particularly the Global Cybersecurity Index, his study illustrates how underinvestment and political divergence have impeded the development of robust defense capabilities. He further advocates for the formation of a dedicated National Cybersecurity Agency, positing that such an entity could address deficits in coordination, incident response, and technical readiness.

Legal fragmentation is also evident in comparative regional analyses, as shown by Elizalde Castañeda, Flores Ramírez, and Castro Lorzo, who explore the legislative trajectories of Chile, Mexico, and Colombia with respect to cybercrime statutes and compliance with the Budapest Convention.[18] Their findings indicate that while all three nations have enacted measures to penalize cyber sabotage, espionage, and other digital offenses, significant disparities persist, particularly in Mexico's and Chile's integration of international standards. Colombia's more robust adherence highlights the need for harmonized reforms to bolster transnational cooperation against cyber threats.

Within Mexico, significant heterogeneity exists at the subnational level. Alcalá Casillas and Meléndez Ehrenzweig reveal considerable inconsistency in how Mexico's 32 states codify cyber offenses—ranging from

---

[15] Andrés Díaz Gómez, *El Delito Informático, Su Problemática y la Cooperación Internacional como Paradigma de su Solución: El Convenio de Budapest*, 8 REDUR 169, 203 (2010).

[16] Hiram Raúl Piña Libién, *Cibercriminalidad y ciberseguridad en México*, 2 IUS COMITIALIS 47–69 (Dec. 2019).

[17] Juan Manuel Aguilar Antonio, *Presente y futuro de los retos de la ciberseguridad en México, una propuesta para la seguridad nacional*, 13 REV. LEGIS. ESTUD. SOC. & OPINIÓN PÚBLICA 83, 120 (2020).

[18] Rodolfo Rafael Elizalde Castañeda, Héctor Hugo Flores Ramírez et al., *Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho Comparado*, 4 IUS COMITIALIS 252, 276 (2021).

fraud to cyberstalking, ultimately undermining an integrated national response.[19] These discrepancies manifest in divergent definitions, penalties, and enforcement protocols. As a result, not only does it become challenging to investigate such crimes uniformly, but the lack of coherent statutory language also erodes both preventative measures and prosecutorial efficacy across the country.

Extending the discussion to include legislative proposals, Aguilar Antonio and Quechol Maciel survey cybersecurity bills introduced in Mexico from 2019 to 2023, revealing a predominantly state-centric, security-oriented paradigm.[20] They argue that human rights considerations, collaborative mechanisms between the public and private sectors, and avenues for international cooperation remain comparatively underexplored. This critique resonates with concurrent findings by Aguirre Quezada, who acknowledges that despite multiple proposals during the LXIV Legislature, the regulatory framework remains inadequate.[21] Drawing on national and international cybersecurity indices, Aguirre Quezada warns that escalating threats—from data breaches to large-scale attacks—necessitate not merely robust laws but also an integrative policy agenda, one that foregrounds human rights and systematically engages diverse stakeholders.

A more recent strand of scholarship examines how cybersecurity shortfalls intersect with broader digital rights. Fuentes-Penna, Gómez-Cárdenas, and González-Ibarra contend that Mexico's regulatory apparatus remains splintered across various statutes, such as the Federal Criminal Code and laws pertaining to national security, generating a legal vacuum that fails to account for human rights nuances in the cyber domain.[22] Although policy documents like the National Cybersecurity Strategy stresses values of transparency and cross-sectoral collaboration, the authors note that legislative codifications have thus far emphasized punitive mechanisms rather than preventative or rights-based approaches.

---

[19] Alcalá Casillas, Miryam Georgina & Meléndez Ehrenzweig, Miguel Ángel, *Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas*, 13 Paakat: Rev. Tecnol. & Soc. 1, 37 (2023)

[20] Juan Manuel Aguilar Antonio & Kate Quechol Maciel, *¿Qué necesita una ley de ciberseguridad? Análisis de las propuestas legislativas en México (2019-2023)*, 28 Paakat: Revista de Tecnología y Sociedad 1, 53 (2023).

[21] Juan Pablo Aguirre Quezada, *Ciberseguridad, desafío para México y trabajo legislativo*, Cuaderno de Investigación No. 87 (Instituto Belisario Domínguez, Senado de la República 2022). http://bibliodigitalibd.senado.gob.mx/handle/123456789/5551.

[22] Alejandro Fuentes Penna & Raúl Gómez-Cárdenas et. al., *La Ciberseguridad en México y los derechos humanos en la era digital*, 24 Espacios Públicos 119, 142 (2023).

From an international trade perspective, Becerril situates cybersecurity within the broader context of free trade agreements, arguing that digital interconnectivity has heightened the imperative for robust cybersecurity standards.[23] She conceptualizes cyberspace as a space of flows, where transactions transcend national boundaries and necessitate regulatory harmonization. Her analysis reinforces the proposition that cybersecurity must be integrated within a multi-stakeholder framework, one that balances national security goals, the preservation of critical infrastructures, and the facilitation of seamless cross-border digital commerce.

Despite the breadth of scholarly inquiry, the literature collectively underscores two primary lacunae in Mexico's cybersecurity landscape: (1) fragmented statutory efforts, compounded by the conflation of cybersecurity measures with those addressing cybercrime, cyber intelligence, and national security; and (2) political inertia that hinders the creation of a centralized, comprehensive cybersecurity law. While existing research has done much to illuminate the prevalence of legislative piecemeal efforts and the tension between security and civil liberties, relatively fewer studies have systematically examined how these fragmented statutes, and the political dynamics that sustain them, produce tangible gaps in enforcement, readiness, and international collaboration.

Accordingly, this article adds to the extant scholarship by providing an in-depth assessment of Mexico's fragmented regulatory fabric, scrutinizing how misalignment among diverse legislative initiatives impedes a cohesive national cybersecurity framework. In contrast to earlier works, it delves explicitly into the underlying political factors that forestall consensus, and explores the ramifications of deferring international norms, such as those embedded in the Budapest Convention and the newly adopted United Nations Convention against Cybercrime. By focusing on the legislative, political, and diplomatic dimensions, this study advances a more nuanced understanding of the barriers to adopting a comprehensive cybersecurity law in Mexico, thereby offering policy-relevant insights that go beyond enumerating statutory provisions to propose a targeted roadmap for reform.

[23] Anahiby Becerril, *La ciberseguridad en los Tratados de Libre Comercio: El comercio electrónico como habilitador para el fortalecimiento de la ciberseguridad internacional*, 8 Revista Chilena de Derecho y Tecnologías, No. 2 111–137 (2019).

IV. Problem and Possible Solutions

Despite recent advances in legislative initiatives, Mexico's cybersecurity framework remains marked by a core problem: fragmentation. Cybersecurity provisions are dispersed across an array of general and sector-specific laws, many of which primarily address national security, criminal offenses, or data protection. This dispersal has led to several operational drawbacks. First, cybersecurity efforts are often conflated with objectives more aligned to cybercrime or intelligence gathering, diluting the focus required for preventive and protective cyber measures. Second, gaps and inconsistencies persist in implementing protocols for threat detection, coordinated response, and infrastructure resilience. Since each piece of legislation is enacted by different authorities and addresses its own set of urgent concerns, the overall framework struggles to establish consistent definitions, standardized best practices, or clear lines of accountability. Lastly, political factors have repeatedly stalled or thwarted the creation of a single, robust cybersecurity law, weakening the country's ability to respond swiftly to sophisticated cyber threats.

A further complication arises from limited coordination among the various stakeholders required to mount an effective cybersecurity strategy. Although several proposals for comprehensive cybersecurity bills have been introduced, disagreements over data privacy safeguards, surveillance powers, and human rights protections often prevent legislative consensus. This lack of alignment not only hampers interagency cooperation but also undermines private-sector engagement, especially among small and medium-sized enterprises that lack the resources to navigate a patchwork of overlapping laws. As a result, Mexico's cybersecurity readiness remains uneven and vulnerable to emerging threats, including identity-based intrusions, large-scale data breaches, and disruptive attacks on critical infrastructure.

Several solutions can help overcome these structural and political obstacles. First, enacting a dedicated cybersecurity law, one that explicitly demarcates cybersecurity from cybercrime and national security, would provide the clarity needed to harmonize standards and definitions across sectors. Such legislation should outline clear roles, responsibilities, and enforcement mechanisms while avoiding overreach into domains where privacy and due process rights might be jeopardized. Second, strengthening institutional coordination through the establishment of a central cybersecurity authority or agency would streamline incident reporting, facilitate capacity-building efforts, and foster more effective interagen-

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

cy collaboration. Third, aligning with international standards and best practices, particularly those embedded in the Budapest Convention and the newly adopted United Nations Convention against Cybercrime, would bolster Mexico's capacity to combat transnational cyber threats and enable it to leverage global expertise. This alignment could include adopting enhanced protocols for cross-border data sharing, electronic evidence preservation, and rapid response measures.

In addition to legal and institutional reforms, multi-stakeholder engagement is crucial, because collaborative platforms that bring together government agencies, private-sector leaders, civil society organizations, and international partners can promote the exchange of best practices, refine threat intelligence, and elevate public awareness. Also, comprehensive workforce development and cybersecurity training should be prioritized to address the human capital gaps that currently limit incident response and policy implementation.

Investments in specialized education, professional certifications, and research funding would help cultivate a skilled workforce capable of supporting both public and private cybersecurity needs. By coupling this emphasis on talent development with well-defined legislative and institutional frameworks, Mexico can move beyond piecemeal reforms, achieving a resilient and adaptive cybersecurity environment that not only meets current challenges but is also prepared for those yet to emerge.

V. Historical Context and Legislative Evolution of Cybersecurity Initiatives in Mexico

Several legislative initiatives and reforms have been proposed in the country over the years to address cybersecurity and cybercrime. These efforts have included amendments to various secondary laws, such as the National Security Law, Federal Criminal Code, Data Protection Law, and even the Federal Constitution. While these reforms represent essential steps toward integrating cybersecurity within Mexico's legal framework, they remain scattered across multiple regulatory areas, lacking a cohesive approach. In this context, special laws specifically dedicated to cybersecurity have been introduced, aiming to provide a more comprehensive regulatory structure. Below is a chronological analysis of these key legislative proposals, highlighting their scope and impact.

1) October 22, 2015. Initiative for the Federal Law to Prevent and Punish Cybercrimes: Senator Omar Fayad Meneses introduced a comprehensive

legislative project aimed at criminalizing cyber offenses.[24] The proposal, known as the *Ley Federal para Prevenir y Sancionar los Delitos Informáticos*, sought to establish clear definitions and penalties for various cybercrimes.

2) March 19, 2019. Law of Information Security and Amendments to the Federal Criminal Code: Senator Jesús Lucía Trasviña Waldenrath presented an initiative to establish the *Ley de Seguridad Informática,*[25] alongside amendments to Title IX of the Federal Criminal Code. This law sought to unify regulations on cyber offenses while establishing an information security framework.
3) September 1, 2020. Initiative for the General Cybersecurity Law: Backed by the entire parliamentary group, this proposal, led by Senator Miguel Ángel Mancera, aimed to create a *Ley General de Ciberseguridad.*[26] This initiative suggested amendments to the Criminal Code, the National Security Law, and the General Law of the National Public Security System. It emphasized the need for an integrated cybersecurity strategy.
4) October 19, 2020. National Cybersecurity Law Proposal: Deputy Javier Salinas Narváez from the Morena party introduced the *Ley Nacional de Seguridad en el Ciberespacio.*[27] The proposal focused on regulating cybersecurity practices within critical national infrastructure, emphasizing national security implications.
5) March 25, 2021. General Cybersecurity Law Initiative: Senator Jesús Lucía Trasviña Waldenrath presented another initiative for a *Ley General de Ciberseguridad*, aiming to consolidate and update existing regulations in the Criminal Code.[28]
6) October 6, 2022. General Cybersecurity Law Proposal: Deputy Juanita Guerra Mena, also from Morena, introduced a new *Ley General de Ciberseguridad*[29] designed to establish unified standards for cybersecurity practices across sectors.

---

[24] Omar Fayad, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal para Prevenir y Sancionar los Delitos Informáticos*, Senado de la República, LXIII Legislatura, Gaceta Parlamentaria, 22 de octubre de 2015 (Mex.).

[25] Jesús Lucía Trasviña Waldenrath, *Iniciativa con Proyecto de Decreto por el que se Reforman y Derogan Diversas Disposiciones del Título Noveno, Libro Segundo del Código Penal Federal y se Expide la Ley de Seguridad Informática*, Senado de la República, LXIV Legislatura, Gaceta Parlamentaria, 19 de marzo de 2019 (Mex.).

[26] Miguel Ángel Mancera Espinosa, *Iniciativa con Proyecto de Decreto por el que se Modifica la Denominación del Capítulo II, del Título Noveno, del Libro Segundo y se Reforma el Artículo 211 bis 1 y se Derogan Diversos Artículos del Código Penal Federal, y se Expide la Ley General de Ciberseguridad*, Senado de la República, LXIV Legislatura, Gaceta Parlamentaria, 1 de septiembre de 2020 (Mex.).

[27] Javier Salinas Narváez, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Nacional de Seguridad en el Ciberespacio*, Cámara de Diputados, LXIV Legislatura, Gaceta Parlamentaria, 19 de octubre de 2020 (Mex.).

[28] Jesús Lucía Trasviña Waldenrath, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley General de Ciberseguridad y se Derogan Diversas Disposiciones del Código Penal Federal*, Senado de la República, LXIV Legislatura, Gaceta Parlamentaria, 25 de marzo de 2021 (Mex.).

[29] Juanita Guerra Mena, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley General de*

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

7) April 25, 2023. Federal Cybersecurity Law Proposal: Proposed by Deputy Javier Joaquín López Casarín from the PVEM, this initiative aimed to implement specific cybersecurity measures within the public and private sectors.[30] This *Ley Federal de Ciberseguridad* presented a detailed framework, but faced logistical challenges and was eventually withdrawn on March 13, 2024.
8) February 8 and April 26, 2023. General Law for the National Digital Security System: Introduced by Deputy Salvador Caro Cabrera of Movimiento Ciudadano, this bill sought to create a L*ey General del Sistema Nacional de Seguridad Digital.*[31] The first version was withdrawn shortly after, and a revised version was presented on April 26.
9) February 14, 2024. Federal Cybersecurity Law Proposal: Senators Checo Pérez Flores and Rafael Espino de la Peña introduced a proposal to repeal existing cybercrime articles in the Criminal Code, replacing them with a comprehensive *Ley Federal de Ciberseguridad.*[32]
10) February 27, 2024. General Cybersecurity Law Proposal: Presented again by Deputy Juanita Guerra Mena, this initiative represents Morena's continued efforts to establish a *Ley General de Ciberseguridad.*[33]
11) March 20, 2024. Federal Cybersecurity Law Proposal: Deputy Javier Joaquín López Casarín reintroduced a revised version of his *Ley Federal de Ciberseguridad,*[34] aiming to address previous criticisms and streamline cybersecurity governance.
12) August 14, 2024. Federal Cybersecurity and Digital Trust Law: Senator Alejandra Lagunes Soto Ruíz from the PVEM presented the *Ley Federal de Ciberseguridad y Confianza Digital,*[35] expanding cybersecurity efforts to include digital trust provisions. This law aims to enhance public confidence in digi-

---

Ciberseguridad, Cámara de Diputados, LXV Legislatura, Gaceta Parlamentaria, 6 de octubre de 2022 (Mex.).

[30] Javier Joaquín López Casarín, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal de Ciberseguridad*, Cámara de Diputados, LXV Legislatura, Gaceta Parlamentaria, 25 de abril de 2023 (Mex.).

[31] Salvador Caro Cabrera, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley General del Sistema Nacional de Seguridad Digital*, Cámara de Diputados, LXV Legislatura, Gaceta Parlamentaria, 6 de diciembre de 2023 (Mex.).

[32] Checo Pérez Flores & Rafael Espino de la Peña, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal de Ciberseguridad y se Derogan los Artículos 211 bis 1–7 del Código Penal Federal*, Senado de la República, LXV Legislatura, Gaceta Parlamentaria, 14 de febrero de 2024 (Mex.).

[33] Juanita Guerra Mena, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley General de Ciberseguridad*, Cámara de Diputados, LXV Legislatura, Gaceta Parlamentaria, 27 de febrero de 2024 (Mex.).

[34] Javier Joaquín López Casarín, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal de Ciberseguridad*, Cámara de Diputados, LXV Legislatura, Gaceta Parlamentaria, 20 de marzo de 2024 (Mex.).

[35] Alejandra Lagunes Soto Ruíz, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal de Ciberseguridad y Confianza Digital y se Reforman Diversas Disposiciones en Materia de Ciberdelitos*, Senado de la República, LXV Legislatura, Gaceta Parlamentaria, 14 de agosto de 2024 (Mex.).

tal infrastructure and includes updates to cybercrime definitions, marking the latest effort to create a holistic cybersecurity policy in Mexico.

13) December 10, 2024. General Citizen Cybersecurity Law: Senator Jesús Lucía Trasviña Waldenrath of the Morena Parliamentary Group introduced a draft decree to enact the General Citizen Cybersecurity Law while repealing several provisions of the Federal Criminal Code.[36] This legislative initiative is designed to modernize Mexico's cybersecurity framework by establishing comprehensive legal measures that protect citizens' digital rights and strengthen coordinated national efforts against emerging cyber threats, marking a significant advancement in the country's overall digital security policy.

14) March 4, 2025. General Cybersecurity Law: Senator Mauricio Vila Dosal of the National Action Party introduced a draft decree to enact the General Cybersecurity Law.[37] This initiative seeks to create a comprehensive legal framework to address the growing cybersecurity challenges in Mexico by protecting digital infrastructure, ensuring the security of personal data, and modernizing the nation's legal response to emerging cyber threats, thereby reinforcing national cybersecurity across public and private sectors.

Despite their differences, these initiatives share several common elements that reveal legislative priorities regarding cybersecurity. One recurring theme across all proposals is the protection of critical infrastructure, underscoring the need to safeguard essential services within an increasingly interconnected digital environment. Additionally, all initiatives seek to strengthen the Criminal Code by incorporating specific cybercrimes and establishing penalties for offenses such as unauthorized access, digital fraud, and data theft. However, each initiative approaches these issues differently: some advocate for stricter penalties, while others propose more measures that are moderate aligned with international best practices. Another shared aspect is the acknowledgment of human rights within the digital sphere, although each proposal varies in its approach to privacy and freedom of expression protections. While some include detailed safeguards to prevent abuse, others have faced criticism for lacking effective privacy protections.

[36] Jesús Lucía Trasviña Waldenrath, Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Ciberseguridad Ciudadana y se derogan diversas disposiciones del Código Penal Federal, Senado de la República, LXVI Legislatura, Gaceta Parlamentaria, 10 de diciembre de 2024 (Mex.).

[37] Mauricio Vila Dosal, Iniciativa con Proyecto de Decreto por el que se expide la *Ley General en materia de Ciberseguridad*, Senado de la República, LXVI Legislatura, Gaceta Parlamentaria, 04 de marzo 2025 (Mex.).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

Significant divergences in approach and focus emerge among the initiatives. For example, Senator Mancera's 2020 proposal advocates for a comprehensive law covering not only cybercrimes but also infrastructure protection and digital rights. In contrast, other proposals, such as those led by Deputy Juanita Guerra Mena and Deputy Javier Joaquín López Casarín in 2023, focus on establishing a specific cybersecurity framework without extending to broader regulatory issues. Moreover, recent initiatives like Senator Alejandra Lagunes' 2024 proposal explicitly seek alignment with international standards, referencing frameworks such as the Budapest Convention on Cybercrime and other global standards. This approach contrasts with previous proposals that focus solely on a national regulatory framework without adopting international principles or practices, reflecting differing perspectives on global cooperation in cybersecurity.

The recurrence of similar initiatives highlights persistent challenges and criticisms that have hindered progress toward a comprehensive cybersecurity law in Mexico. One primary obstacle has been the lack of consensus regarding privacy safeguards, a recurring point of contention between legislators and civil society. Many proposals have been perceived as overly intrusive due to insufficient provisions for protecting privacy and preventing abuse, especially in terms of surveillance and control over digital communications. Another major challenge lies in the lack of clarity surrounding implementation and oversight mechanisms, raising questions about the practical feasibility of these laws. Lastly, extensive amendments to the Criminal Code have faced opposition due to concerns that broad and vague definitions of cybercrimes could criminalize legitimate online behavior, thereby affecting citizens' rights.

In conclusion, this chronological and thematic analysis of Mexico's cybersecurity legislative initiatives reveals a continuous effort to address digital threats, but a unified and consensus-driven approach remains elusive. Each legislative attempt reflects both the growing importance of cybersecurity within the country and the complex balance required to secure the nation while respecting fundamental rights in the digital realm. Progress toward an effective and comprehensive cybersecurity law likely depends on closer collaboration among legislators, civil society, and the private sector to design a framework that addresses the complexities of Mexico's digital landscape and is practically enforceable, while respecting the privacy and rights of citizens.

VI. Comprehensive Overview of Cybersecurity Provisions in Mexican Legislation

Within Mexico's legislative framework, cybersecurity is addressed through specific provisions in federal laws and codes, establishing a robust legal foundation to tackle challenges related to information security, access control, and privacy in digital environments. These legal instruments seek to safeguard digital security and data integrity by defining and penalizing cybercrimes, regulating public security practices, and setting standards for personal data management. Below, we make a review of key articles that address cybersecurity from criminal, organizational, and fundamental rights perspectives.

The Federal Criminal Code (*Código Penal Federal*)[38] includes significant provisions addressing cybercrimes explicitly linked to digital or electronic means. Articles 199 Septies, 202, 202 BIS, 210-211 bis 7, 254 bis 1, and 424 bis II outline offenses such as the solicitation of minors via digital communication, child pornography, and unauthorized disclosure of private information. Article 199 Septies criminalizes the solicitation of sexual material from minors through digital channels, while Article 202 penalizes the production, distribution, and exhibition of child pornography. Articles 210 and 211 address the unlawful disclosure of private information, with Article 211 Bis focusing on breaches involving intercepted private communications. Additionally, Article 254 bis 1 penalizes actions that obstruct investigations by altering or destroying electronic files, while Article 424 bis II sanctions the manufacture of devices intended to bypass digital protections on software, thus reinforcing the legal response to cybercrimes.

The National Guard Law (*Ley de la Guardia Nacional*)[39] grants cybersecurity authority to the National Guard, particularly in Article 9, sections XXVI and XXXVIII. This law allows the National Guard to request mobile device geolocation and other information from telecommunications providers, subject to judicial authorization, to prevent criminal activities. It also enables monitoring of public internet networks to deter online crimes, with judicial decisions required within twelve hours for any requests, reflecting a balance between operational effectiveness and respect for privacy.

---

[38] Código Penal Federal [C.P.F.] [Federal Criminal Code], as amended, *Diario Oficial de la Federación* [D.O.F.], 14 de agosto de 1931 (Mex.).

[39] Ley de la Guardia Nacional [L.G.N.] [National Guard Law], *Diario Oficial de la Federación* [D.O.], 27 de mayo de 2019 (Mex.).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

The Federal Police Law (*Ley de la Policía Federal*)[40] also provides specific cybersecurity measures. Articles 8 (XXVIII, XXIX, XLII) and 48-55 allow the Federal Police to request information from telecommunications providers, intercept communications (under judicial authorization), and conduct surveillance of public internet spaces to prevent crime. These provisions impose strict procedural controls and monthly reporting requirements, underscoring the legal and regulatory safeguards necessary for cybersecurity operations.

The Internal Security Law (*Ley de Seguridad Interior*)[41] establishes provisions to preserve internal security and promote intelligence gathering while respecting human rights. Articles 4 (VII) and 29-31 define intelligence as the collection and processing of data, with federal and armed forces authorized to gather information legally. The law mandates mechanisms for inter-agency collaboration, with the aim to safeguard national security while protecting fundamental rights, illustrating an approach that balances national security needs with respect for individual freedoms.

The National Security Law *(Ley de Seguridad Nacional)*[42] has a dedicated focus on information security, with specific protocols for handling confidential government information. Articles 6 (V), 8 (IV), 9, 10, 13 (VII), 19 (VIII and IX), 33-55, 61-64, 70, and 71 (V) establish rules for the classification and protection of sensitive information. This law emphasizes confidentiality in national security operations, regulates communication interception during national security threats, and includes requirements for the acquisition and management of specialized technology. The provisions in this law emphasize the importance of data integrity and confidentiality within national security.

The Federal Law Against Organized Crime (*Ley Federal contra la Delincuencia Organizada*)[43] addresses information security within organized crime investigations, particularly in Articles 8, 11 bis 1, 16-21, 24, and 26-28. Judicial authorization is required for communication interceptions, electronic surveillance, and the use of informants. The law mandates severe

---

[40] Ley de la Policía Federal [L.P.F.] [Federal Police Law], *Diario Oficial de la Federación* [D.O.], 1 de junio de 2009 (Mex.).

[41] Ley de Seguridad Interior [L.S.I.] [Internal Security Law], *Diario Oficial de la Federación* [D.O.], 21 de diciembre de 2017 (Mex.).

[42] Ley de Seguridad Nacional [L.S.N.] [National Security Law], *Diario Oficial de la Federación* [D.O.], 31 de enero de 2005 (Mex.).

[43] Ley Federal contra la Delincuencia Organizada [L.F.C.D.O.] [Federal Law Against Organized Crime], as amended, *Diario Oficial de la Federación* [D.O.], 7 de noviembre de 1996 (Mex.).

penalties for unauthorized interventions by public officials, highlighting the commitment to upholding data integrity and privacy in the context of organized crime while balancing investigation efficacy with individual rights.

The Federal Law on Private Security (*Ley Federal de Seguridad Privada*)[44] regulates private security activities, emphasizing the importance of data security. Articles 2 (I, XIV, XV), 15 (IV and V), 32 (XXII), and 45-50 define data security as maintaining confidentiality, integrity, and availability through security systems and information backups. The law grants the General Directorate authority to approve private security services, including electronic monitoring and establishes confidentiality requirements for private security providers.

The General Law on Women's Access to a Life Free of Violence (*Ley General de Acceso de las Mujeres a una Vida Libre de Violencia*)[45] tackles digital violence in Articles 20 Quater, 20 Quinquies, and 20 Sexies. This law defines digital violence as any malicious action using technology to disseminate intimate content without consent, with corresponding penalties in the Federal Criminal Code. Additionally, it addresses media violence, requiring protective measures against the unauthorized disclosure of digital content involving women, including legal obligations for digital platforms to assist in content removal.

The General Law of the National Public Security System (*Ley General del Sistema Nacional de Seguridad Pública*)[46] addresses information security protocols, particularly regarding public security databases. Key provisions are found in Articles 5 (II), 7 (XII), 31 (VIII), 39 (B.XIV), 108 (IV), 110, 139 (I, II, III), 144 (I), and 150. This law mandates cellular and radio signal blocking in detention facilities, enforces confidentiality in public security records, and requires real-time data sharing across security entities. These provisions reinforce the integrity of the National Public Security Information System and outline requirements for private security services, including licensing and compliance with local regulations.

The General Law to Prevent, Punish, and Eradicate Crimes of Human Trafficking (*Ley General Para Prevenir, Sancionar y Erradicar los Delitos en Ma-*

---

[44] Ley Federal de Seguridad Privada [L.F.S.P.] [Federal Law on Private Security], *Diario Oficial de la Federación* [D.O.], 6 de julio de 2006 (Mex.).

[45] Ley General de Acceso de las Mujeres a una Vida Libre de Violencia [L.G.A.M.V.L.V.] [General Law on Women's Access to a Life Free of Violence], *Diario Oficial de la Federación* [D.O.], 1 de febrero de 2007 (Mex.).

[46] Ley General del Sistema Nacional de Seguridad Pública [L.G.S.N.S.P.] [General Law of the National Public Security System], *Diario Oficial de la Federación* [D.O.], 2 de enero de 2009 (Mex.).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

teria de Trata de Personas)[47] establishes comprehensive information security measures in Articles 16, 32, 33, 88 (IV.d), 113 (XVII), 118, and 119 (IV). This law mandates strict confidentiality protocols for electronically stored data related to trafficking investigations and victim assistance programs, with exclusive federal authority for data collection, protection, and exchange. These provisions highlight the commitment to data security in human trafficking cases, ensuring victim protection and secure handling of sensitive information.

The General Law to Prevent and Punish Kidnapping (*Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro*)[48] reinforces information security in public safety contexts, specifically through Articles 16, 24, 25, 30, 40 (XIX), and 43 (X). This law includes penalties for public officials who disclose confidential information without justification and mandates telecommunications providers to support investigations. The law also calls for permanent communication restrictions in detention centers and facilitates cooperation between investigative units and telecom providers, illustrating the importance of public-private partnerships in cybersecurity for crime prevention.

The National Law on Criminal Execution (*Ley Nacional de Ejecución Penal*)[49] establishes data security principles in the penitentiary system, with a focus on prisoner information confidentiality. Articles 4 (6), 40 (IX), 41 (V), 60, 136, 137, 154, and 171 (III) prevent unauthorized telecommunications use in correctional facilities and impose sanctions proportionate to data security breaches. This law mandates ethical handling of medical and judicial records, reinforcing the integrity of data management in non-custodial measures.

The National Detention Registry Law (*Ley Nacional del Registro de Detenciones*)[50] mandates secure management of personal data related to detainees. Key articles include 9, 10, 13-16, 26-29, 32, and 35, which outline security protocols for personal data storage, requiring restricted access and digital authentication. The law imposes sanctions for breach-

---

[47] Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos [L.G.P.S.E.D.M.T.P.] [General Law to Prevent, Punish, and Eradicate Crimes of Human Trafficking], *Diario Oficial de la Federación* [D.O.], 14 de junio de 2012 (Mex.).

[48] Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro [L.G.P.S.D.M.S.] [General Law to Prevent and Punish Kidnapping], *Diario Oficial de la Federación* [D.O.], 30 de noviembre de 2010 (Mex.).

[49] Ley Nacional de Ejecución Penal [L.N.E.P.] [National Law on Criminal Execution], *Diario Oficial de la Federación* [D.O.], 16 de junio de 2016 (Mex.).

[50] Ley Nacional del Registro de Detenciones [L.N.R.D.] [National Detention Registry Law], *Diario Oficial de la Federación* [D.O.], 27 de mayo de 2019 (Mex.).

es, and mandates technological security measures in data registries, ensuring detainee data management aligns with national data protection standards.

The Federal Law on the Protection of Personal Data Held by Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*)[51] sets forth rigorous standards for personal data protection in Articles 3, 18-20, 39, 55, 58, and in Chapter XII (Articles 62-64). These provisions mandate that data controllers implement comprehensive administrative, technical, and physical security measures to safeguard personal data against damage, loss, alteration, destruction, or unauthorized access, taking into account existing risks, data sensitivity, and technological developments. In addition, data breach notifications are required immediately when security vulnerabilities significantly affect the economic or moral rights of data subjects, as specified in Article 19, while Article 20 obliges both controllers and third parties involved in data processing to maintain confidentiality throughout and beyond the processing stages.

The law further empowers the Ministry, under Article 39, to disseminate international security standards and best practices, and Article 55 authorizes the Ministry to access necessary documentation during verification procedures under strict confidentiality obligations. Infractions, such as compromising database security or breaching confidentiality requirements as outlined in Article 58, are subject to penalties, with Chapter XII imposing criminal sanctions that include prison terms from three months to three years for profit-driven breaches (Article 62), six months to five years for deceptive practices intended for illicit gain (Article 63), and doubled penalties when sensitive personal data is involved (Article 64). Overall, this law aims to ensure the secure and responsible management of personal data within Mexico's digital landscape.

The General Law on the Protection of Personal Data Held by Obliged Entities (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*)[52] establishes a comprehensive framework for ensuring the confidentiality, integrity, and availability of personal data within public institutions. Articles 3, 24-36, 53, 58, 78, and 132 collectively outline detailed requirements that include the development of a security document, defin-

[51] Ley Federal de Protección de Datos Personales en Posesión de los Particulares [L.F.P.D.P.P.P.] [Federal Law on Protection of Personal Data Held by Private Parties], *Diario Oficial de la Federación* [D.O.F.], 20 de marzo de 2025 (Mex.).

[52] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [L.G.P.D.P.S.O.] [General Law on Protection of Personal Data Held by Obligated Subjects], *Diario Oficial de la Federación* [D.O.F.], 26 de enero de 2017 (Mex.).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

ing key concepts such as administrative, physical, and technical security measures, and mandate continuous risk analysis, gap assessments, and the implementation of corrective actions. The law requires periodic reviews and updates of these measures to address evolving technological challenges and emerging threats, while enforcing strict confidentiality obligations on all personnel involved in data processing. Additionally, it regulates contractual relationships with data processors and empowers Transparency Committees to oversee compliance, with clearly defined penalties for non-compliance, including misclassification of data and breaches of confidentiality. Overall, these provisions provide a robust legal foundation for proactive data protection and responsible information management in the public sector.

The General Transparency and Access to Public Information Law (*Ley General de Transparencia y Acceso a la Información Pública*)[53] establishes a robust legal framework that guarantees the human right to access information held by public entities while simultaneously instituting rigorous protocols for classifying and safeguarding sensitive data. Articles 4, 39, 46, 107, 112, 119, 20, 102, 110, and 115-119 delineate a balanced approach that not only ensures the broad dissemination of public information but also imposes strict measures, such as the formation of Transparency Committees, the mandatory application of a damage test to assess potential harm to public interest or national security, and detailed classification procedure, to protect information deemed reserved or confidential. This framework upholds transparency and accountability while mitigating risks to national security, public safety, and individual rights, thereby reinforcing an effective system of public information management.

The General Law of Archives (*Ley General de Archivos*)[54] focuses on document management and data security, particularly in Articles 5, 25, 41, 46 (IV), and 60-63. Public institutions are required to implement technical and administrative measures to preserve document integrity, availability, and accessibility. For electronic records, this law emphasizes the importance of annual security programs and the comprehensive management of digital documentation, including access assignment, storage, and traceability. The law further mandates secure third-party services and cloud document management, with strict requirements to ensure

[53] Ley General de Transparencia y Acceso a la Información Pública [L.G.T.A.I.P.] [General Law of Transparency and Access to Public Information], *Diario Oficial de la Federación* [D.O.F.], 20 de marzo de 2025 (Mex.).

[54] Ley General de Archivos [L.G.A.] [General Law on Archives], *Diario Oficial de la Federación* [D.O.F.], 15 de junio de 2018 (Mex.).

the authenticity, integrity, and security of information. These protocols underscore the law's commitment to a secure and efficient digital record-keeping environment.

The Credit Institutions Law (*Ley de Instituciones de Crédito*)[55] outlines critical security requirements for multiple banking institutions, particularly in Articles 10, 46 bis, 77, 96, 110 bis 11, and 115 (c). It commands operational plans incorporating security measures, emphasizing internal controls and physical security at office facilities, and authorizes electronic notifications. The law also highlights client information protection, internal compliance areas, and imposes financial penalties for breaches, especially for unauthorized disclosures of information, stressing the importance of information security in the financial sector.

The Credit Institutions Law establishes foundational security requirements for banking institutions, covering operational plans, internal controls, physical security, client information protection, and financial penalties for breaches. Complementing this, the *Disposiciones de Carácter General Aplicables a las Instituciones de Crédito*[56] acts as a formal administrative instrument with legislative weight, addressing areas often unregulated by traditional laws and mandating robust requirements that enhance financial sector resilience. This circular imposes comprehensive obligations, including stringent credit risk management protocols, capital adequacy guidelines, transparency via risk disclosures, and periodic reporting obligations. It further dictates stringent governance and internal controls by clarifying institutional responsibilities and enforcing the separation of duties. The circular also includes mandatory incident reporting measures: incidents impacting information security, such as breaches, must be reported to the Commission within 48 hours. Moreover, banks are obligated to notify customers about data breaches involving personal information to mitigate risk exposure. Additionally, the Chief Information Security Officer (CISO) must be kept informed monthly of security risks, ensuring proactive oversight and enforcement of security measures within the institution.

The Law of Insurance and Bonding Institutions (*Ley de Instituciones de Seguros y de Fianzas*)[57] addresses information security in Articles 41 (V.g),

[55] Ley de Instituciones de Crédito [L.I.C.] [Credit Institutions Law], *Diario Oficial de la Federación* [D.O.F.], 18 de julio de 1990 (Mex.).

[56] Disposiciones de Carácter General Aplicables a las Instituciones de Crédito [Circular Única de Bancos], *Diario Oficial de la Federación* [D.O.F.], 2 de marzo de 2004, última reforma DOF 31 de diciembre de 2021, arts. 115, 116, 117.

[57] Ley de Instituciones de Seguros y de Fianzas [L.I.S.F.] [Insurance and Bonding Institutions Law], *Diario Oficial de la Federación* [D.O.F.], 4 de abril de 2013 (Mex.).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

268 (I), 269, 366 (XXXVII), 468, and 492 (c). During the authorization process, a comprehensive activity plan with specific security measures is required to preserve information integrity. While institutions may outsource services, they must follow strict confidentiality guidelines. The Commission, with technical autonomy, may share information with foreign financial authorities through reciprocal agreements, provided there is no associated risk. Provisions for electronic notification with acknowledgment of receipt also enhance the information security protocols.

The Payments System Law (*Ley de Sistemas de Pagos*),[58] particularly in Articles 6 (V) and 19-21, emphasizes that payment systems' internal regulations should ensure both efficiency and security under the Bank of Mexico's authorization. Security measures for operating systems and contingency plans are mandatory, while the Bank of Mexico supervises and assesses risk control systems, enforcing compliance where necessary. Administrators are required to provide information to validate adherence, and the Bank of Mexico can implement mandatory adjustment programs to rectify deficiencies, ensuring transaction security. Additionally, two important circulars further strengthen cybersecurity and IT requirements for payment systems: Circular 12/2023,[59] applicable to the *Sistema de Pagos Electrónicos Interbancarios* (SPEI), and Circular 13/2023,[60] which governs the *Sistema de Pagos Interbancarios en Dólares* (SPID).

The Credit Unions Law (*Ley de Uniones de Crédito*)[61] sets forth provisions in Articles 17 (IV), 121 (IV), 129 (III), and 142. This law requires that authorization requests include operational plans addressing security to preserve information integrity. It penalizes the destruction of information to obstruct supervision with prison sentences, mandates the security of data relating to partner identification and operations, and allows for electronic notifications with acknowledgment, contingent upon security protocols, stressing secure electronic communication.

The Securities Market Law (*Ley del Mercado de Valores*)[62] integrates information security standards in the financial sector, particularly for broker-

[58] Ley de Sistemas de Pagos [L.S.P.] [Payment Systems Law], *Diario Oficial de la Federación* [D.O.F.], 21 de diciembre de 2002 (Mex.).

[59] Circular 12/2023, Diario Oficial de la Federación [D.O.F.], 22 de noviembre de 2023 (Mex.), https://www.dof.gob.mx/nota_detalle.php?codigo=5709192&fecha=22/11/2023#gsc.tab=0.

[60] Circular 13/2023, Diario Oficial de la Federación [D.O.F.], 22 de noviembre de 2023 (Mex.), https://www.dof.gob.mx/nota_detalle.php?codigo=5709193&fecha=22/11/2023#gsc.tab=0.

[61] Ley de Uniones de Crédito [L.U.C.] [Credit Unions Law], *Diario Oficial de la Federación* [D.O.], 13 de agosto de 1993 (Mex.).

[62] Ley del Mercado de Valores [L.M.V.] [Securities Market Law], *Diario Oficial de la Feder-*

age firms and stock exchanges, in Articles 115 (III.b), 177, 212 (III.c), 220 (II.c), 226 Bis (V), 235 (III.c), 245, 282, and 392 (II.n). This law requires detailed operational plans focusing on information integrity, data confidentiality mechanisms, and third-party agreements with robust security policies. Additionally, the law enforces preventive and detection obligations to curb financial crimes, imposing sanctions for non-compliance, thus safeguarding trust and information integrity within the securities market.

The General Law of Credit Organizations and Auxiliary Activities (*Ley General de Organizaciones y Actividades Auxiliares del Crédito*),[63] with provisions in Articles 87-D (I.p, II.k, III.c, IV.p), 95 (c), 95 bis (c), and 101 bis 12, highlights cybersecurity protocols in auxiliary credit organizations. It requires authorization from the Ministry of Finance to proceed with criminal charges for certain offenses and mandates strict security of customer identification data. Electronic notifications are permitted if agreed to in writing and via secure systems defined by financial authorities, underscoring cybersecurity's role in credit organizations.

The General Law of Commercial Companies (*Ley General de Sociedades Mercantiles*)[64] specifies requirements for security in corporate events, in Articles 6 (XIV) and 245. It permits electronic, optical, or other technological means for participation, provided they ensure real-time interaction equivalent to physical meetings. This law also commands secure mechanisms for attendee access, identification verification, and vote recording. For document preservation, liquidators may retain records in digital or print formats, following digitization guidelines set by the Ministry of Economy to ensure information integrity.

The General Law of Credit Instruments and Operations (*Ley General de Títulos y Operaciones de Crédito*),[65] particularly in Articles 432-435, addresses financial crimes related to information security. It penalizes the unauthorized production, alteration, and misuse of credit cards and sensitive data, and restricts unauthorized access to electronic systems of issuing entities. This regulatory approach seeks to protect information security,

ación [D.O.F.], 30 de diciembre de 2005 (Mex.).

63 Ley General de Organizaciones y Actividades Auxiliares del Crédito [L.G.O.A.A.C.] [General Law on Credit Organizations and Auxiliary Activities], *Diario Oficial de la Federación* [D.O.], 14 de enero de 1985 (Mex.).

64 Ley General de Sociedades Mercantiles [L.G.S.M.] [General Law of Commercial Companies], *Diario Oficial de la Federación* [D.O.F.], 4 de agosto de 1934 (Mex.).

65 Ley General de Títulos y Operaciones de Crédito [L.G.T.O.C.] [General Law of Negotiable Instruments and Credit Operations], *Diario Oficial de la Federación* [D.O.F.], 27 de agosto de 1932 (Mex.).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

prevent fraudulent manipulation, and safeguard users from illicit activities in the financial sector.

The Law for the Transparency and Regulation of Financial Services (*Ley para la Transparencia y Ordenamiento de los Servicios Financieros*),[66] particularly in Article 4 Bis 3 (I.c) and 22 (II.b), focuses on financial service regulation with an emphasis on data security. It highlights the joint responsibility of the National Banking and Securities Commission and the Bank of Mexico in regulating transaction networks, enforcing security and operational requirements, and underlining the role of digital signatures and security protocols for data integrity in digital financial services.

The Law to Regulate the Activities of Cooperative Savings and Loan Societies (*Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo*),[67] particularly in Articles 62, 72 (III), 110 (III and IV), and 129, grants the Commission authority to supervise internal and information control systems. It emphasizes the security of partner and transaction data, imposing prison sentences and fines for supervision obstruction. Electronic notifications with acknowledgment are permitted under secure and explicitly agreed-upon conditions, reinforcing the confidentiality and integrity of information in cooperative societies.

The Law to Regulate Financial Groups (*Ley Para Regular las Agrupaciones Financieras*),[68] in Articles 39 (V), 52 (V-VII), 59 (IX), 106, 114, 128, 157 (V-VII), and 173, outlines key information security requirements. It establishes the board's responsibility to oversee risk and accounting systems, prohibits tampering with financial records, and mandates that directors ensure system integrity. The law grants the Supervisory Commission unrestricted access to facilities and documentation and imposes penalties, including imprisonment, for unlawful activities involving financial information. Electronic notifications are permitted, further fortifying security in official communication channels.

The Law to Regulate Financial Technology Institutions (*Ley para Regular las Instituciones de Tecnología Financiera*),[69] in Articles 34 (IV), 37 (III), 39

---

[66] Ley para la Transparencia y Ordenamiento de los Servicios Financieros [L.T.O.S.F.] [Transparency and Financial Services Law], *Diario Oficial de la Federación* [D.O.F.], 18 de julio de 2007 (Mex.).

[67] Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo [L.R.A.S.C.A.P.] [Law to Regulate the Activities of Cooperative Savings and Loan Societies], *Diario Oficial de la Federación* [D.O.F.], 13 de agosto de 2009 (Mex.).

[68] Ley Para Regular las Agrupaciones Financieras [L.R.A.F.] [Law to Regulate Financial Groups], *Diario Oficial de la Federación* [D.O.F.], 18 de julio de 1990 (Mex.).

[69] Ley para Regular las Instituciones de Tecnología Financiera [L.R.I.T.F.] [Law to Regulate Financial Technology Institutions], *Diario Oficial de la Federación* [D.O.F.], 9 de marzo de 2018 (Mex.).

(VI), 48, 56, 58 (III), 76, 83 (III), 87 (II), 103 (IV.b), 119, 128, 130-133, and 142, focuses on security measures in fintech institutions. It mandates robust infrastructure, effective internal controls, and clear communication on the risks associated with virtual asset transactions. Furthermore, advanced electronic signature standards are enforced to maintain legal validity. Specific sanctions for misconduct underscore protections against unauthorized access and system integrity breaches, allowing for electronic acknowledgment for secure communication.

The Law to Regulate Credit Information Societies (*Ley para Regular las Sociedades de Información Crediticia*),[70] particularly in Articles 7 (V), 17 bis, 22, 32, 33, 37, 38, 52, and 62 (II), imposes stringent data security measures within the credit information sector. This law addresses IT systems and control measures, ensuring confidentiality post-employment, and emphasizes secure data exchanges with authorities, user authentication, and security guidelines. Penalties, including significant fines, are enforced for improper handling of credit information, emphasizing cybersecurity's critical role in this sector.

The Commercial Code (*Código de Comercio*)[71] incorporates significant provisions regarding information security, particularly in Articles 20, 30 bis, 93 bis, 97, 99, 101, 102 (II), and 1390 Bis 26. It mandates that the Public Registry of Commerce operate electronically, managed through a specialized program by the Secretariat, with a strong focus on data security. Access to the database is facilitated by digital certificates, emphasizing the integrity and preservation of electronic messages. Additionally, the code stipulates requirements for advanced electronic signatures, detailing the signer's responsibilities and setting guidelines for certification service providers. Electronic recording of hearings is also permitted jn order to ensure fidelity and information integrity. These provisions highlight the need for robust digital security measures to secure commercial transactions and public records.

The Foreign Trade Law (*Ley de Comercio Exterior*),[72] particularly in Articles 17 A and 20 A, requires that compliance with non-tariff restrictions and regulations in international trade be documented with secure, preferably electronic, measures. The law acknowledges electronic signatures certi-

[70] Ley para Regular las Sociedades de Información Crediticia [L.R.S.I.C.] [Law to Regulate Credit Information Societies], *Diario Oficial de la Federación* [D.O.F.], 15 de enero de 2002 (Mex.).

[71] Código de Comercio [CÓD.COM.] [Commercial Code], as amended, *Diario Oficial de la Federación* [D.O.F], 7 de octubre de 1889 (Mex.).

[72] Ley de Comercio Exterior [L.C.E.] [Foreign Trade Law], *Diario Oficial de la Federación* [D.O.], 27 de julio de 1993 (Mex.).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

fied by accredited providers, facilitating transactions and notifications related to non-tariff regulations and established programs. This approach enhances the security of electronic transactions and ensures the authenticity of documentation in foreign trade.

The Federal Consumer Protection Law (*Ley Federal de Protección al Consumidor*),[73] in Articles 1 (VIII), 76 bis, and 76 bis 1, focuses on promoting and protecting consumer rights, with a dedicated chapter on electronic transactions. Regarding information security, the law sets out measures to ensure consumer data confidentiality, including a prohibition on dissemination without explicit consent. Suppliers are required to use technical safeguards to protect information and must disclose these mechanisms to consumers before transactions occur. The law emphasizes transparency in commercial practices, mandating clear communication of terms and conditions to consumers, and prohibits deceptive practices. Furthermore, it specifies requirements for suppliers using electronic means, including adherence to security standards, verification mechanisms, proof support, and protection of consumers' personal information.

The National Code of Civil and Family Procedures (*Código Nacional de Procedimientos Civiles y Familiares*),[74] specifically Articles 142 (IV), 918, 934, and 964-973, provides guidelines on information security within judicial contexts and digital technology usage. It grants jurisdictional authorities the ability to restrict physical or digital access during judicial hearings to those who do not adhere to safety and cybersecurity measures. Digital submission and transfer of files for appellate proceedings are also permitted, ensuring data confidentiality and integrity. Chapter III is dedicated to digital justice systems and information security, mandating robust cybersecurity measures and appointing individuals to supervise and correct potential digital system issues. Sections I and II emphasize security protocols to prevent unauthorized access and detail responsibilities for jurisdictional authorities, highlighting the significance of information security as a guiding principle.

The National Code of Criminal Procedure (*Código Nacional de Procedimientos Penales*)[75] covers Articles 51, 71, 131 (II), 291-303, and 444, allowing electronic means across procedural stages, including online reporting

---

[73] Ley Federal de Protección al Consumidor [L.F.P.C.] [Federal Consumer Protection Law], *Diario Oficial de la Federación* [D.O.F.], 24 de diciembre de 1992 (Mex.).

[74] Código Nacional De Procedimientos Civiles Y Familiares [C.N.P.C.F.] [National Civil and Family Procedure Code], *Diario Oficial de la Federación* [D.O.F.], 7 de junio de 2022 (Mex.).

[75] Código Nacional de Procedimientos Penales [C.N.P.P.] [National Code of Criminal Procedure], *Diario Oficial de la Federación* [D.O.F.], 5 de marzo de 2014 (Mex.).

and videoconferencing. The code validates certified electronic copies and permits the replacement of originals with electronic files, enabling the Public Prosecutor's Office to accept reports digitally. It includes provisions for private communication interception, emphasizing authenticity and the destruction of non-relevant records. The code also regulates service provider cooperation and confidentiality regarding internationally obtained information.

The Federal Fiscal Code (*Código Fiscal de la Federación*),[76] in Articles 17-C to 17-L, 29 (VI), 38, 75 (II)(g), 82-G, 85 (IV), 87 (IV), 105 (XV), 110 (IV, VI), 111 (VI), 111 bis (II, III, V), and 134 (I), contains strict information security regulations for tax matters, enforcing advanced electronic signatures certified by the SAT (*Servicio de Administración Tributaria*). It defines protocols for identity validation, digital seal certificates, revocation conditions, and SAT's certification services, promoting security in electronic transactions. In addition, it dictates issuing online digital tax receipts with specific computational requirements, ensuring authenticity and certificate validity, and outlines penalties for infractions, including unauthorized handling of digital tax receipts and confidential information breaches by public officials.

The General Law of Institutions and Electoral Procedures (*Ley General de Instituciones y Procedimientos Electorales*),[77] in Articles 329, 341, and 343, specifies security requirements for overseas voting by Mexican citizens, particularly through electronic voting systems. It emphasizes the reliability and security of the voting process, ensuring freedom and secrecy. The law stipulates electronic voting criteria such as auditability, pre-vote verification, coercion prevention, unique voter identification, and real-time electoral results. Notably, certain provisions were revalidated on March 2, 2023, after being deemed unconstitutional in a SCJN ruling on June 23, 2023.

The General Law of Electoral Remedies (*Ley General de los Medios de Impugnación en Materia Electoral)*[78] in Article 6 (5) mandates the Federal Electoral Tribunal to implement an online judicial system, allowing for electronic submission and processing of appeals. It highlights advanced electronic

[76] Código Fiscal de la Federación [C.F.F.] [Federal Tax Code], as amended, *Diario Oficial de la Federación* [D.O.F.], 31 de diciembre de 1981 (Mex.).

[77] Ley General de Instituciones y Procedimientos Electorales [L.G.I.P.E.] [General Law of Electoral Institutions and Procedures], *Diario Oficial de la Federación* [D.O.F.], 23 de mayo de 2014 (Mex.).

[78] Ley General de los Medios de Impugnación en Materia Electoral [L.G.M.I.M.E.] [General Law of Electoral Remedies], *Diario Oficial de la Federación* [D.O.F.], 23 de mayo de 2014 (Mex.).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

signatures' legal validity as substitutes for handwritten ones and allows for the attachment of authenticated electronic files. The focus is on secure procedural communication, ensuring that electronic mechanisms comply with legal requirements for authenticity and integrity.

The Federal Law for the Protection of Industrial Property (*Ley Federal de Protección a la Propiedad Industrial*),[79] Articles 22-24, 163-169, 386 (XIV), and 402 (III-VI), governs information security, especially public access to registry information, with exceptions for confidential requests. Title Three defines and protects Trade Secrets, recognizing them as confidential information conferring competitive advantages. The law commands confidentiality safeguards, regulates unauthorized acquisition of trade secrets, and imposes penalties for breaches, including in judicial and administrative contexts, thereby securing trade secrets and enforcing data security.

The Federal Copyright Law (*Ley Federal del Derecho de Autor*),[80] Articles 101-114, 114 Bis to 114 Octies, 231 (V, VII), and 232 Quinquies, addresses information security for software and databases. It safeguards proprietary rights over software, permitting technological protection measures and regulating rights management. The law imposes responsibilities on Internet Service Providers (ISPs) for information security, stipulating measures to prevent copyright and related rights infringements. It prohibits importing or using devices that disable protections, thereby strengthening security for software and databases and establishing ISP responsibilities for preventing copyright violations.

The Customs Law (*Ley Aduanera*),[81] particularly Articles 4 (II)(c-e), 14-C, 14-D, 16, 16-A, 16-B, 16-D, 59 (III), 100-A (VII), 121 (I)(c), 135-A, 144 (XXXV), 160 (X), 167-F (VII), and 185 (VIII), mandates the acquisition and maintenance of surveillance equipment, automated systems, and control measures within strategic locations, such as ports and airports. It also imposes security standards, electronic controls, and secure data transmission protocols for customs operations like electronic pre-validation of declarations and management within strategic fiscal zones. The law protects data integrity in customs processing, establishing penalties for security breaches, and underscoring the importance of secure customs information handling.

---

[79] Ley Federal de Protección a la Propiedad Industrial [L.F.P.P.I.] [Federal Law on Industrial Property Protection], *Diario Oficial de la Federación* [D.O.F.], 1 de julio de 2020 (Mex.).

[80] Ley Federal del Derecho de Autor [L.F.D.A.] [Federal Copyright Law], as amended, *Diario Oficial de la Federación* [D.O.F.], 24 de diciembre de 1996 (Mex.).

[81] Ley Aduanera [L.A.] [Customs Law], as amended, *Diario Oficial de la Federación* [D.O.F.], 15 de diciembre de 1995 (Mex.).

The Federal Labor Law (*Ley Federal del Trabajo*),[82] Articles 330-E (V, VIII), 721, 776 (VIII), and 836-A to 836-D, addresses data security in remote work by requiring employers to implement data protection measures for telework arrangements. Specific provisions cover digital evidence admissibility and procedural actions via electronic means, introducing terms such as certifying authority, digital certificate, and electronic signature. Detailed regulations govern electronic evidence handling, including designating official experts and requirements for digital document submission and retrieval, highlighting concerns over data security and authenticity in labor and judicial contexts.

The Amparo Law (*Ley de Amparo*),[83] Article 30, sets protocols for secure judicial notifications via electronic means, requiring digital signatures to verify authenticity. It includes secure handling procedures for digital documents, daily system checks, and defined timeframes. The law permits notifications by court officers for heightened security in certain cases, addressing system interruptions by pausing legal deadlines to ensure data integrity.

The Civil Aviation Law (*Ley de Aviación Civil*),[84] Articles 78 bis to 78 Bis 11, emphasizes operational safety, entrusting the Federal Civil Aviation Agency (AFAC) with security oversight. Service providers must implement certified safety management systems with risk assessment and continuous improvement processes. AFAC's certification depends on regulatory compliance, emphasizing data confidentiality and use limitations for operational purposes. International cooperation on data sharing is also highlighted.

The Advanced Electronic Signature Law (*Ley de Firma Electrónica Avanzada*),[85] Articles 8 (II, III, V, VI), 13, 14, 16 (II, III), 19, 22, 25, and 27, covers security aspects of electronic signatures. It establishes principles of authenticity, integrity, non-repudiation, and confidentiality, and requires entities to create secure electronic systems with access controls. Public access to electronic data and documents is allowed unless classified. Procedures for document replacement with electronic equivalents are defined,

---

[82] Ley Federal del Trabajo [L.F.T.] [Federal Labor Law], as amended, *Diario Oficial de la Federación* [D.O.F.], 1 de abril de 1970 (Mex.).

[83] Ley de Amparo, Reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos [L.A.] [Amparo Law], *Diario Oficial de la Federación* [D.O.F.], 2 de abril de 2013 (Mex.).

[84] Ley de Aviación Civil [L.A.C.] [Civil Aviation Law], *Diario Oficial de la Federación* [D.O.F.], 12 de mayo de 1995 (Mex.).

[85] Ley de Firma Electrónica Avanzada [L.F.E.A.] [Advanced Electronic Signature Law], *Diario Oficial de la Federación* [D.O.F.], 11 de enero de 2012 (Mex.).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

with revocation conditions and responsibilities for certificate holders and certifying authorities. The law allows inter-entity coordination to standardize technology, ensuring secure and authentic digital signatures.

The Federal Telecommunications and Broadcasting Law (*Ley Federal de Telecomunicaciones y Radiodifusión*),[86] Articles 3 (XXXII), 145 (III), 181, 189-190 bis, 191 (II), 197, and 298 (D)(V), implements robust information security measures, such as user data privacy protections, data retention requirements for service providers, and collaboration with security and justice authorities. Key provisions include a georeferenced database, content blocking upon user request, and sanctions for breaching confidentiality and communication privacy measures. The Supreme Court of Justice recently nullified changes related to the National Mobile User Registry, which mandated biometric and personal data collection, finding that it violated proportionality, as alternatives existed to ensure public safety without compromising privacy.

The General Education Law (*Ley General de Educación*),[87] Articles 74 (III, IV, V, VIII), 78, 85, 113 (VII), and 115 (XIII), promotes information security within educational settings, including measures to counter cyberbullying. It mandates psychosocial support, legal guidance, and free advisory mechanisms for involved parties, with a digital safety agenda focused on responsible technology use. It holds parents and educators accountable for promoting safe digital practices and issues guidelines for secure technology use by educational authorities.

The General Law on the Rights of Children and Adolescents (*Ley General de los Derechos de Niñas, Niños y Adolescentes*),[88] Articles 57 (XX), 77, 81, 101 Bis 2, 103 (XI), and 149, integrates information security by promoting quality education that encourages safe technology use. The law recognizes minors' rights to secure internet access, providing measures to protect their privacy in electronic media. Additionally, it mandates that educators impart responsible technology use, with penalties for privacy violations against minors, safeguarding their personal information in the digital realm.

---

[86] Ley Federal de Telecomunicaciones y Radiodifusión [L.F.T.R.] [Federal Telecommunications and Broadcasting Law], *Diario Oficial de la Federación* [D.O.F.], 14 de julio de 2014 (Mex.).

[87] Ley General de Educación [L.G.E.] [General Education Law], *Diario Oficial de la Federación* [D.O.F.], 13 de septiembre de 2019 (Mex.).

[88] Ley General de los Derechos de Niñas, Niños y Adolescentes [L.G.D.N.N.A.] [General Law on the Rights of Children and Adolescents], *Diario Oficial de la Federación* [D.O.F.], 4 de diciembre de 2014 (Mex.).

The General Health Law (*Ley General de Salud*),[89] Articles 53 Bis, 74 Ter (VIII), 103 Bis 3, and 109 Bis, addresses information security in healthcare by authorizing service providers to use biometric and electronic records for user identification. It ensures health information confidentiality, mandates specific genetic data protections, requires explicit consent for genome studies, and entrusts the Ministry of Health with issuing guidelines for electronic health record systems, emphasizing security and interoperability across National Health System institutions.

In summary, the Mexican legal framework on cybersecurity reflects a comprehensive approach, combining criminal, regulatory, and public security provisions to address the complexities of digital security in a rapidly evolving landscape. By delineating specific offenses, establishing data protection standards, and empowering public security entities, these laws work in tandem to strengthen the integrity, confidentiality, and resilience of Mexico's digital infrastructure. While certain laws indirectly protect information security or cybersecurity in Mexico, it is both imperative and critically necessary to establish a dedicated cybersecurity law. This section has illustrated the current fragmented state of Mexico's approach; however, this fragmentation is not ideal. On the contrary, a unified law and specialized authorities are essential for cohesive and effective governance in this domain. Although legal goods related to cybersecurity and cybercrime have been mentioned here for pedagogical purposes, a cybersecurity law should focus specifically on cybersecurity itself, rather than on overlapping areas such as cybercrime. As cyber threats continue to evolve, a focused approach is required to underscore the country's commitment to safeguarding personal data, protecting public safety, and ensuring accountability within digital ecosystems.

VII. Relevant International Cybersecurity Treaties Involving Mexico: Ratified and Pending

Mexico's involvement in international cybersecurity treaties underscores its commitment to global security standards and collaborative approaches to countering digital threats. Through a combination of ratified treaties and active participation in negotiations for prospective agreements, Mexico is progressively aligning its cybersecurity framework with international norms. This alignment enhances Mexico's capacity to address

[89] Ley General de Salud [L.G.S.] [General Health Law], *Diario Oficial de la Federación* [D.O.F.], 7 de febrero de 1984 (Mex.).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

and mitigate cyber risks on a global scale, enabling both domestic and cross-border resilience against cyber threats. In this section, we analyze key international treaties involving Mexico, with particular focus on those with binding cybersecurity provisions and those in which Mexico holds a significant position as a signatory or observer.

The Budapest Convention on Cybercrime (2001)[90] stands as the sole binding international instrument specifically dedicated to combating cybercrime. It aims to harmonize national laws related to cybercrime and provide a framework for international cooperation. The Convention mandates the criminalization of offenses against the confidentiality, integrity, and availability of computer systems and data. It also establishes procedural laws that facilitate cooperation across jurisdictions in cybercrime investigations. Although Mexico holds observer status, its involvement in the Convention indicates a commitment to aligning its cybersecurity practices with internationally accepted standards. Adopting these standards could enhance Mexico's capacity to collaborate in global cybercrime investigations and set a foundation for potential future ratification.

Moreover, two protocols complement the Budapest Convention, expanding its reach in addressing cybercrime more comprehensively. The Additional Protocol to the Convention on Cybercrime (2003) targets the criminalization of acts of a racist and xenophobic nature committed through computer systems.[91] This protocol provides measures to counteract online hate speech, ensuring that cybercrime frameworks extend to protect individuals and groups from racial and xenophobic propaganda distributed via digital channels. The Second Additional Protocol to the Convention on Cybercrime (2022) focuses on enhanced cooperation and the disclosure of electronic evidence,[92] a crucial aspect of cybercrime investigations. This protocol emphasizes the importance of international collaboration and outlines processes for rapidly accessing electronic data, facilitating timely and effective responses to cyber incidents across borders.

---

[90] Convention on Cybercrime, opened for signature Nov. 23, 2001, 41 I.L.M. 282 (entered into force July 1, 2004).

[91] Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, opened for signature Jan. 28, 2003, ETS No. 189 (entered into force Mar. 1, 2006).

[92] Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence, opened for signature May 12, 2022, CETS No. 224.

The United States-Mexico-Canada Agreement (USMCA),[93] or T-MEC in Spanish, which came into effect in 2020, includes provisions specifically related to cybersecurity in Chapter 19 on Digital Trade. These provisions aim to enhance data protection, promote cybersecurity cooperation, and encourage a risk-based approach to cybersecurity across North America. Article 19.15 of the USMCA explicitly emphasizes the development of response capabilities, information-sharing practices, and trust-building measures in digital trade through enhanced cybersecurity. By aligning its cybersecurity efforts with those of its primary trading partners, the USMCA strengthens Mexico's internal cybersecurity mechanisms and its cross-border defenses, reinforcing the region's collective resilience against digital threats.

The United Nations Convention against Cybercrime, adopted by the General Assembly on 24 December 2024 in New York by resolution 79/243, represents the first comprehensive global treaty dedicated to addressing cybercrime.[94] Developed over nearly three years of negotiations and having been unanimously approved by UN Member States, the Convention provides States with a broad range of measures to prevent and combat cybercrime while aiming to strengthen international cooperation in sharing electronic evidence for serious crimes. During its negotiation, strong statements from Australia, Canada, the European Union, Liechtenstein, New Zealand, Switzerland, the United Kingdom, and particularly the United States underscored the necessity of integrating human rights safeguards. Meanwhile, the UN Office on Drugs and Crime (UNODC), serving as the substantive secretariat, continues to highlight the Convention's pivotal role in bolstering international cooperation, capacity-building, and rapid response mechanisms, while cautioning against the potential misuse of even well-structured treaties by authoritarian regimes.

Mexico's government has warmly welcomed the adoption of this Convention, highlighting its importance in setting a global standard for cybersecurity and international cooperation.[95] Mexico's active role in the negotiation process emphasized human rights protections, transparen-

---

[93] Agreement Between the United States of America, the United Mexican States, and Canada, 19 U.S.C. § 4501 (entered into force July 1, 2020).

[94] G.A. Res. 79/243, U.N. GAOR, 79th Sess., Agenda Item 108, U.N. Doc. A/RES/79/243 (Dec. 31, 2024)

[95] Secretaría de Relaciones Exteriores, Mexican Government Welcomes Adoption of UN Convention Against Cybercrime, Press Release No. 303 (Aug. 9, 2024), https://www.gob.mx/sre/prensa/mexican-government-welcomes-adoption-of-un-convention-against-cybercrime.

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

cy, and inclusivity. Mexican representatives participated constructively throughout the sessions, contributing to a robust legal instrument aimed at effectively combating cybercrime on a global scale. The Convention also supports Mexico's goals for international regulatory harmonization and legislative advancement in cybersecurity. This treaty, once ratified by Member States, will establish a unified legal framework to tackle cyber threats, closing gaps in national legislation and enhancing global cybersecurity collaboration.

In summary, Mexico's active participation in these international treaties and its commitment to aligning with global cybersecurity norms reflect a proactive approach to addressing the complex and evolving challenges of the digital age. By engaging with these treaties, Mexico not only bolsters its national cybersecurity infrastructure but also contributes to a coordinated international response to cyber threats, reinforcing collective global security.

VIII. Results and Discussion

The analysis of Mexico's cybersecurity regulatory landscape reveals a persistent fragmentation that significantly hinders the country's ability to protect its digital infrastructure, users` personal data and the citizens` economic interests. Our review of legislative proposals and existing laws shows that cybersecurity provisions remain scattered across multiple statutes, largely focused on cybercrime, cyber intelligence, and national security, rather than consolidated in a singular, comprehensive instrument. This lack of cohesion is consistently identified as a principal obstacle to effective governance and coordination, ultimately impeding the prompt detection, mitigation, and prosecution of cyber threats.

A central finding is that the proliferation of disparate bills, many of which overlap or conflict with one another, has produced gaps in coverage and enforcement. Despite numerous initiatives, from the first Federal Law to Prevent and Punish Cybercrimes in 2015 to the latest General or Federal Cybersecurity proposals in 2025, none has achieved the political consensus required to pass comprehensive cybersecurity legislation. This legislative deadlock has left Mexico reliant on piecemeal reforms in criminal, national security, and data protection laws, none of which fully address the preventive, protective, and resilience-oriented dimensions of cybersecurity. The net effect is a system where the lines between cybersecurity, cybercrime, and broader national security measures are blurred,

complicating interagency collaboration and diluting the focused attention that a dedicated cybersecurity framework demands.

Compounding the legislative fragmentation are political and institutional factors that stymie swift and decisive action. As evidenced by multiple withdrawn or stalled bills, partisan disagreements and divergent priorities across legislative factions have repeatedly obstructed the establishment of a unifying legal framework. In several of the proposals examined, tensions arose over the appropriate scope of surveillance powers, concerns about human rights safeguards, and the extent to which domestic law should incorporate, or deviate from, international instruments such as the Budapest Convention and the newly adopted United Nations Convention against Cybercrime. Consequently, the absence of a strong cross-party commitment to cybersecurity has stalled legal reforms and limited robust investments in cybersecurity infrastructure, leaving key sectors, including SMEs, underprepared for sophisticated cyber incursions.

Despite these systemic shortcomings, there have been incremental gains. Certain legislative initiatives, including those referencing international standards and treaties, underscore a growing recognition of the need for cross-border collaboration. Mexico's observer status in the Budapest Convention, its alignment with USMCA provisions on digital trade, and its vocal support for the new UN Cybercrime Convention highlight a willingness to align domestic legislation with global cybersecurity norms. These moves reflect an evolving consensus that international partnerships, backed by interoperable legal frameworks, are critical to addressing the transnational nature of cyber threats. Furthermore, statistical indicators, such as Mexico's upward movement in the Global Cybersecurity Index, suggest that incremental policy improvements and targeted investments in specialized cyber units are having some effect, although cooperation measures still lag behind legal and organizational efforts.

Taken together, these findings highlight an urgent need to replace the current patchwork of cybersecurity provisions with a cohesive, purpose-built cybersecurity law. Such a framework must clearly demarcate cybersecurity from cybercrime and national security concerns and incorporate robust governance mechanisms to coordinate interagency efforts, promote public-private collaboration, and elevate the country's readiness against evolving cyber threats. Political consensus, buttressed by continued progress toward harmonizing with international standards, emerges as the linchpin for sustainable reform. In this context, the discussion

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

underscores that while incremental legislative and institutional changes have yielded modest improvements, the core challenge persists: only a unified and well-structured cybersecurity regime can effectively address Mexico's rising threat landscape.

IX. Limitations and Future Research

Despite offering a detailed examination of Mexico's fragmented cybersecurity regulatory environment, this study is subject to several limitations. First, the research primarily relies on legislative and policy documents, along with secondary data from international indices and official reports. While these sources provide substantial insight into the legal framework and broader policy directions, they do not capture the lived realities of enforcement, the day-to-day practices of governmental agencies, or the perspectives of private-sector actors, especially small and medium-sized enterprises (SMEs). Future work could incorporate interviews, case studies, and ethnographic field research to more fully represent the practical challenges and successes of implementing cybersecurity provisions at multiple levels of governance.

A second limitation arises from the dynamic nature of Mexican cybersecurity legislation. This article captures a snapshot of proposed and existing laws, many of which are subject to rapid change, withdrawal, or amendment due to political negotiations. Given the evolving policy landscape, there is a risk of legal obsolescence shortly after publication. Ongoing legislative developments and fluctuating political support underscore the necessity for continuous monitoring. More frequent updates or longitudinal research designs would help track these legislative shifts over time and assess the stability and impact of enacted measures.

Third, although the analysis covers diverse sectors, from financial services and telecommunications to education and electoral processes, it does not systematically evaluate how each sector adopts and adapts cybersecurity measures on an operational level. Sector-specific assessments could illuminate how fragmentation influences resilience, resource allocation, and inter-agency coordination in practice. Future studies may also investigate the interplay between federal policies and state-level initiatives, given that Mexico's federal system often generates a complex mosaic of subnational regulations.

Building on these limitations, future research agendas might benefit from three main directions. First, empirical investigations on how cyber-

security laws translate into tangible outcomes, such as reduced cyber incidents or higher compliance rates, would strengthen the evidence base for legislative reforms. Second, comparative analyses with countries that have recently adopted comprehensive cybersecurity laws could yield best practices and highlight pathways for Mexico to achieve political consensus. Finally, an interdisciplinary approach that integrates technological, legal, and sociopolitical perspectives would foster a more holistic understanding of cybersecurity challenges, further informing both policy design and implementation in this critical domain.

X. Conclusions

This study aimed to demonstrate that, despite incremental legislative advances and increased policy attention, Mexico's cybersecurity framework remains primarily constrained by fragmentation. Existing statutes, ranging from the Federal Criminal Code to sector-specific financial regulations, address distinct aspects of cyber risk without forming a cohesive regime. The dispersion of regulations across multiple domains, cybercrime, data protection, national security, has created overlapping mandates and inconsistencies, ultimately undermining enforcement efficacy and interagency coordination. Moreover, persistent political hurdles and divergences in legislative priorities have impeded the passage of a consolidated cybersecurity law, leaving vital sectors such as critical infrastructure and small and medium-sized enterprises (SMEs) inadequately protected against escalating cyber threats.

By tracing the trajectory of cybersecurity bills proposed between 2015 and 2025, this article reveals recurring themes that have inhibited legislative consensus. Chief among these are debates over surveillance authority, human rights safeguards, and alignment with international instruments such as the Budapest Convention. While the growing willingness to reference these global standards signals an emerging recognition of cybercrime's transnational nature, integrating such norms into domestic law requires sustained political commitment and well-defined legal frameworks. The absence of broad-based legislative support not only perpetuates legal ambiguity but also discourages the private sector from making robust cybersecurity investments, particularly among SMEs that face unique resource constraints.

Despite these challenges, Mexico has made noticeable strides in certain areas, including incremental enhancements to criminal statutes,

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

targeted intelligence capabilities, and improved ranking in global cybersecurity indices. These gains draw attention to the potential for more comprehensive reforms. A unified cybersecurity law, distinct from cybercrime or intelligence legislation, would streamline disparate statutes, clarify institutional responsibilities, and promote technical guidelines for proactive cyber defense. Institutional reforms that establish a central authority with a clear mandate to oversee cybersecurity initiatives are equally essential, as it will coordinate responses and foster collaboration among federal entities, state governments, and private-sector partners.

A convergent multi-stakeholder approach, anchored in transparent governance, international cooperation, and robust capacity-building is definitely the most viable pathway to bolster national cyber resilience. While incremental legal and policy changes have generated modest improvements, this article's findings reaffirm that only a cohesive and strategically oriented legislative framework can effectively mitigate Mexico's complex cyber risks. Future endeavors should thus concentrate on reconciling political differences, enhancing institutional cooperation, and fortifying alignment with global cybersecurity norms, ensuring that Mexico's digital ecosystem is both resilient and adaptive in an ever-evolving landscape.

XI. References

Accenture, *The Cyber-Resilient CEO*, at 4-5, 18 (2024).

Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, opened for signature Jan. 28, 2003, ETS No. 189 (entered into force Mar. 1, 2006).

Agreement Between the United States of America, the United Mexican States, and Canada, 19 U.S.C. § 4501 (entered into force July 1, 2020).

Alcalá Casillas, Miryam Georgina & Meléndez Ehrenzweig, Miguel Ángel, *Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas*, 13 Paakat: Rev. Tecnol. & Soc. 1, 37 (2023).

Alejandra Lagunes Soto Ruíz, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal de Ciberseguridad y Confianza Digital y se Reforman Diversas Disposiciones en Materia de Ciberdelitos*, Senado de la República, LXV Legislatura, Gaceta Parlamentaria, 14 de agosto de 2024 (Mex.).

Alejandro Fuentes Penna & Raúl Gómez-Cárdenas et. al., *La Ciberseguridad en México y los derechos humanos en la era digital*, *24* Espacios Públicos 119, 142 (2023).

Anahiby Becerril, *La ciberseguridad en los Tratados de Libre Comercio: El comercio electrónico como habilitador para el fortalecimiento de la ciberseguridad internacional*, 8 Revista Chilena de Derecho y Tecnologías 2, 111–137 (2019).

Andrés Díaz Gómez, *El Delito Informático, Su Problemática y la Cooperación Internacional como Paradigma de su Solución: El Convenio de Budapest*, 8 REDUR 169, 203 (2010).

Asociación del Internet de México & Consejo de Datos y Tecnologías Emergentes, *3er Estudio de Ciberseguridad en México 2023*, at 3-4, 6 (2023).

Checo Pérez Flores & Rafael Espino de la Peña, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal de Ciberseguridad y se Derogan los Artículos 211 bis 1–7 del Código Penal Federal*, Senado de la República, LXV Legislatura, Gaceta Parlamentaria, 14 de febrero de 2024 (Mex.).

Circular 12/2023, Diario Oficial de la Federación [D.O.], 22 de noviembre de 2023 (Mex.), https://www.dof.gob.mx/nota_detalle.php?codigo=5709192&fecha=22/11/2023#gsc.tab=0.

Circular 13/2023, Diario Oficial de la Federación [D.O.], 22 de noviembre de 2023 (Mex.), https://www.dof.gob.mx/nota_detalle.php?codigo=5709193&fecha=22/11/2023#gsc.tab=0.

Cisco, *2024 Cybersecurity Readiness Index - Mexico,* at 2-3 (2024).

Código de Comercio [CÓD.COM.] [Commercial Code], as amended, *Diario Oficial de la Federación* [D.O.], 7 de octubre de 1889 (Mex.).

Código Fiscal de la Federación [C.F.F.] [Federal Tax Code], as amended, *Diario Oficial de la Federación* [D.O.], 31 de diciembre de 1981 (Mex.).

Código Nacional De Procedimientos Civiles Y Familiares [C.N.P.C.F.] [National Civil and Family Procedure Code], *Diario Oficial de la Federación* [D.O,], 7 de junio de 2022 (Mex.).

Código Nacional de Procedimientos Penales [C.N.P.P.] [National Code of Criminal Procedure], *Diario Oficial de la Federación* [D.O.], 5 de marzo de 2014 (Mex.).

Código Penal Federal [C.P.F.] [Federal Criminal Code], as amended, *Diario Oficial de la Federación* [DOF], 14 de agosto de 1931 (Mex.).

Convention on Cybercrime, opened for signature Nov. 23, 2001, 41 I.L.M. 282 (entered into force July 1, 2004).

Disposiciones de Carácter General Aplicables a las Instituciones de Crédito [Circular Única de Bancos], *Diario Oficial de la Federación* [D.O.], 2 de marzo de 2004, última reforma DOF 31 de diciembre de 2021, arts. 115, 116, 117.

G.A. Res. 79/243, U.N. GAOR, 79th Sess., Agenda Item 108, U.N. Doc. A/RES/79/243 (Dec. 31, 2024).

Google Cloud, *Cybersecurity Forecast 2024* (2024).

Hiram Raúl Piña Libién, *Cibercriminalidad y ciberseguridad en México*, 2 IUS Comitialis 47–69 (Dec. 2019).

IBM & Ponemon Institute, *Cost of a Data Breach Report 2024*, at 3-4 (2024).

IBM, *X-Force Threat Intelligence Index 2024* (2024).

Inter-American Development Bank, *2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean* (2020).

Inter-American Development Bank, *2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean* (2020).

International Telecommunication Union, *Global Cybersecurity Index 2020*, https://itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (last visited Nov. 11, 2024).

International Telecommunication Union, *Global Cybersecurity Index 2024*, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (last visited Nov. 11, 2024).

Javier Joaquín López Casarín, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal de Ciberseguridad*, Cámara de Diputados, LXV Legislatura, Gaceta Parlamentaria, 25 de abril de 2023 (Mex.).

Javier Joaquín López Casarín, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal de Ciberseguridad*, Cámara de Diputados, LXV Legislatura, Gaceta Parlamentaria, 20 de marzo de 2024 (Mex.).

Javier Salinas Narváez, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Nacional de Seguridad en el Ciberespacio*, Cámara de Diputados, LXIV Legislatura, Gaceta Parlamentaria, 19 de octubre de 2020 (Mex.).

Jesús Lucía Trasviña Waldenrath, *Iniciativa con Proyecto de Decreto por el que se Reforman y Derogan Diversas Disposiciones del Título Noveno, Libro Segundo del Código Penal Federal y se Expide la Ley de Seguridad Informática*, Senado de la República, LXIV Legislatura, Gaceta Parlamentaria, 19 de marzo de 2019 (Mex.).

Jesús Lucía Trasviña Waldenrath, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley General de Ciberseguridad y se Derogan Diversas Disposiciones del Código Penal Federal*, Senado de la República, LXIV Legislatura, Gaceta Parlamentaria, 25 de marzo de 2021 (Mex.).

Jesús Lucía Trasviña Waldenrath, Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Ciberseguridad Ciudadana y se derogan diversas disposiciones del Código Penal Federal, Senado de la República, LXVI Legislatura, Gaceta Parlamentaria, 10 de diciembre de 2024 (Mex.).

Juan Manuel Aguilar Antonio & Kate Quechol Maciel, *¿Qué necesita una ley de ciberseguridad? Análisis de las propuestas legislativas en México (2019-2023)*, 28 Paakat: Revista de Tecnología y Sociedad 1, 53 (2023).

Juan Manuel Aguilar Antonio, *Presente y futuro de los retos de la ciberseguridad en México, una propuesta para la seguridad nacional*, 13 Rev. Legis. Estud. Soc. & Opinión Pública 83, 120 (2020).

Juan Pablo Aguirre Quezada, *Ciberseguridad, desafío para México y trabajo legislativo*, Cuaderno de Investigación No. 87 (Instituto Belisario Domínguez, Senado de la República 2022). http://bibliodigitalibd.senado.gob.mx/handle/123456789/5551.

Juanita Guerra Mena, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley General de Ciberseguridad*, Cámara de Diputados, LXV Legislatura, Gaceta Parlamentaria, 6 de octubre de 2022 (Mex.).

Juanita Guerra Mena, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley General de Ciberseguridad*, Cámara de Diputados, LXV Legislatura, Gaceta Parlamentaria, 27 de febrero de 2024 (Mex.).

Ley Aduanera [L.A.] [Customs Law], as amended, *Diario Oficial de la Federación* [D.O.], 15 de diciembre de 1995 (Mex.).

Ley de Amparo, Reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos [L.A.] [Amparo Law], *Diario Oficial de la Federación* [D.O.], 2 de abril de 2013 (Mex.).

Ley de Aviación Civil [L.A.C.] [Civil Aviation Law], *Diario Oficial de la Federación* [DOF], 12 de mayo de 1995 (Mex.).

Ley de Comercio Exterior [L.C.E.] [Foreign Trade Law], *Diario Oficial de la Federación* [DOF], 27 de julio de 1993 (Mex.).

Ley de Firma Electrónica Avanzada [L.F.E.A.] [Advanced Electronic Signature Law], *Diario Oficial de la Federación* [DOF], 11 de enero de 2012 (Mex.).

Ley de Instituciones de Crédito [L.I.C.] [Credit Institutions Law], *Diario Oficial de la Federación* [DOF], 18 de julio de 1990 (Mex.).

Ley de Instituciones de Seguros y de Fianzas [L.I.S.F.] [Insurance and Bonding Institutions Law], *Diario Oficial de la Federación* [DOF], 4 de abril de 2013 (Mex.).

Ley de la Guardia Nacional [L.G.N.] [National Guard Law], *Diario Oficial de la Federación* [DOF], 27 de mayo de 2019 (Mex.).

Ley de la Policía Federal [L.P.F.] [Federal Police Law], *Diario Oficial de la Federación* [DOF], 1 de junio de 2009 (Mex.).

Ley de Seguridad Interior [L.S.I.] [Internal Security Law], *Diario Oficial de la Federación* [DOF], 21 de diciembre de 2017 (Mex.).

Ley de Seguridad Nacional [L.S.N.] [National Security Law], *Diario Oficial de la Federación* [DOF], 31 de enero de 2005 (Mex.).

Ley de Sistemas de Pagos [L.S.P.] [Payment Systems Law], *Diario Oficial de la Federación* [D.O.F], 21 de diciembre de 2002 (Mex.).

Ley de Uniones de Crédito [L.U.C.] [Credit Unions Law], *Diario Oficial de la Federación* [D.O.], 13 de agosto de 1993 (Mex.).

Ley del Mercado de Valores [L.M.V.] [Securities Market Law], *Diario Oficial de la Federación* [D.O.], 30 de diciembre de 2005 (Mex.).

Ley Federal contra la Delincuencia Organizada [L.F.C.D.O.] [Federal Law Against Organized Crime], as amended, *Diario Oficial de la Federación* [D.O.], 7 de noviembre de 1996 (Mex.).

Ley Federal de Protección a la Propiedad Industrial [L.F.P.P.I.] [Federal Law on Industrial Property Protection], *Diario Oficial de la Federación* [D.O.], 1 de julio de 2020 (Mex.).

Mexican Law Review, New Series, vol. XVIII, num. 1, July - December 2025, pp. 69-115
Jersain Zadamig Llamas Covarrubias
Cybersecurity in México: An In-Depth Analysis of a Fragmented Regulatory Landscape
e-ISSN: 1870-0578 | DOI: https://doi.org/10.22201/iij.24485306e.2025.1.19686

Ley Federal de Protección al Consumidor [L.F.P.C.] [Federal Consumer Protection Law], *Diario Oficial de la Federación* [D.O.], 24 de diciembre de 1992 (Mex.).

Ley Federal de Protección de Datos Personales en Posesión de los Particulares [L.F.P.D.P.P.P.] [Federal Law on Protection of Personal Data Held by Private Parties], *Diario Oficial de la Federación* [D.O.], 20 de marzo de 2025 (Mex.).

Ley Federal de Seguridad Privada [L.F.S.P.] [Federal Law on Private Security], *Diario Oficial de la Federación* [D.O.], 6 de julio de 2006 (Mex.).

Ley Federal de Telecomunicaciones y Radiodifusión [L.F.T.R.] [Federal Telecommunications and Broadcasting Law], *Diario Oficial de la Federación* [D.O.], 14 de julio de 2014 (Mex.).

Ley Federal del Derecho de Autor [L.F.D.A.] [Federal Copyright Law], as amended, *Diario Oficial de la Federación* [D.O.], 24 de diciembre de 1996 (Mex.).

Ley Federal del Trabajo [L.F.T.] [Federal Labor Law], as amended, *Diario Oficial de la Federación* [D.O.], 1 de abril de 1970 (Mex.).

Ley General de Acceso de las Mujeres a una Vida Libre de Violencia [L.G.A.M.V.L.V.] [General Law on Women's Access to a Life Free of Violence], *Diario Oficial de la Federación* [D.O.], 1 de febrero de 2007 (Mex.).

Ley General de Archivos [L.G.A.] [General Law on Archives], *Diario Oficial de la Federación* [D.O.], 15 de junio de 2018 (Mex.).

Ley General de Educación [L.G.E.] [General Education Law], *Diario Oficial de la Federación* [D.O.], 13 de septiembre de 2019 (Mex.).

Ley General de Instituciones y Procedimientos Electorales [L.G.I.P.E.] [General Law of Electoral Institutions and Procedures], *Diario Oficial de la Federación* [D.O.], 23 de mayo de 2014 (Mex.).

Ley General de los Derechos de Niñas, Niños y Adolescentes [L.G.D.N.N.A.] [General Law on the Rights of Children and Adolescents], *Diario Oficial de la Federación* [D.O.], 4 de diciembre de 2014 (Mex.).

Ley General de los Medios de Impugnación en Materia Electoral [L.G.M.I.M.E.] [General Law of Electoral Remedies], *Diario Oficial de la Federación* [D.O.], 23 de mayo de 2014 (Mex.).

Ley General de Organizaciones y Actividades Auxiliares del Crédito [L.G.O.A.A.C.] [General Law on Credit Organizations and Auxiliary Activities], *Diario Oficial de la Federación* [D.O.], 14 de enero de 1985 (Mex.).

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [L.G.P.D.P.S.O.] [General Law on Protection of Personal Data Held by Obligated Subjects], *Diario Oficial de la Federación* [D.O.], 26 de enero de 2017 (Mex.).

Ley General de Salud [L.G.S.] [General Health Law], *Diario Oficial de la Federación* [D.O.], 7 de febrero de 1984 (Mex.).

Ley General de Sociedades Mercantiles [L.G.S.M.] [General Law of Commercial Companies], *Diario Oficial de la Federación* [D.O.], 4 de agosto de 1934 (Mex.).

Ley General de Títulos y Operaciones de Crédito [L.G.T.O.C.] [General Law of Negotiable Instruments and Credit Operations], *Diario Oficial de la Federación* [D.O.], 27 de agosto de 1932 (Mex.).

Ley General de Transparencia y Acceso a la Información Pública [L.G.T.A.I.P.] [General Law of Transparency and Access to Public Information], *Diario Oficial de la Federación* [D.O.], 20 de marzo de 2025 (Mex.).

Ley General del Sistema Nacional de Seguridad Pública [L.G.S.N.S.P.] [General Law of the National Public Security System], *Diario Oficial de la Federación* [D.O.], 2 de enero de 2009 (Mex.).

Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro [L.G.P.S.D.M.S.] [General Law to Prevent and Punish Kidnapping], *Diario Oficial de la Federación* [D.O.], 30 de noviembre de 2010 (Mex.).

Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos [L.G.P.S.E.D.M.T.P.] [General Law to Prevent, Punish, and Eradicate Crimes of Human Trafficking], *Diario Oficial de la Federación* [D.O.], 14 de junio de 2012 (Mex.).

Ley Nacional de Ejecución Penal [L.N.E.P.] [National Law on Criminal Execution], *Diario Oficial de la Federación* [D.O.], 16 de junio de 2016 (Mex.).

Ley Nacional del Registro de Detenciones [L.N.R.D.] [National Detention Registry Law], *Diario Oficial de la Federación* [D.O.], 27 de mayo de 2019 (Mex.).

Ley para la Transparencia y Ordenamiento de los Servicios Financieros [L.T.O.S.F.] [Transparency and Financial Services Law], *Diario Oficial de la Federación* [D.O.], 18 de julio de 2007 (Mex.).

Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo [L.R.A.S.C.A.P.] [Law to Regulate the Activities of Cooperative Savings and Loan Societies], *Diario Oficial de la Federación* [D.O.], 13 de agosto de 2009 (Mex.).

Ley Para Regular las Agrupaciones Financieras [L.R.A.F.] [Law to Regulate Financial Groups], *Diario Oficial de la Federación* [D.O.], 18 de julio de 1990 (Mex.).

Ley para Regular las Instituciones de Tecnología Financiera [L.R.I.T.F.] [Law to Regulate Financial Technology Institutions], *Diario Oficial de la Federación* [D.O.], 9 de marzo de 2018 (Mex.).

Ley para Regular las Sociedades de Información Crediticia [L.R.S.I.C.] [Law to Regulate Credit Information Societies], *Diario Oficial de la Federación* [D.O.], 15 de enero de 2002 (Mex.).

Mauricio Vila Dosal, Iniciativa con Proyecto de Decreto por el que se expide la *Ley General en materia de Ciberseguridad*, Senado de la República, LXVI Legislatura, Gaceta Parlamentaria, 04 de marzo 2025 (Mex.).

Miguel Ángel Mancera Espinosa, *Iniciativa con Proyecto de Decreto por el que se Modifica la Denominación del Capítulo II, del Título Noveno, del Libro Segundo y se Reforma el Artículo 211 bis 1 y se Derogan Diversos Artículos del Código Penal Federal, y se Expide la Ley General de Ciberseguridad*, Senado de la República, LXIV Legislatura, Gaceta Parlamentaria, 1 de septiembre de 2020 (Mex.).

Omar Fayad, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal para Prevenir y Sancionar los Delitos Informáticos*, Senado de la República, LXIII Legislatura, Gaceta Parlamentaria, 22 de octubre de 2015 (Mex.).

Presidencia de la República [Office of the President], Estrategia Nacional de Ciberseguridad [National Cybersecurity Strategy] (2017) (Mex.).

PwC, *Digital Trust Insights 2025 - Mexico Edition* (2025).

Rodolfo Rafael Elizalde Castañeda & Héctor Hugo Flores Ramírez et al., *Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho Comparado*, 4 IUS Comitialis 252, 276 (2021).

Salvador Caro Cabrera, *Iniciativa con Proyecto de Decreto por el que se Expide la Ley General del Sistema Nacional de Seguridad Digital*, Cámara de Diputados, LXV Legislatura, Gaceta Parlamentaria, 6 de diciembre de 2023 (Mex.).

Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence, opened for signature May 12, 2022, CETS No. 224.

Secretaría de Relaciones Exteriores, Mexican Government Welcomes Adoption of UN Convention Against Cybercrime, Press Release No. 303 (Aug. 9, 2024), https://www.gob.mx/sre/prensa/mexican-government-welcomes-adoption-of-un-convention-against-cybercrime.

World Economic Forum, *Global Cybersecurity Outlook 2025* (2025).

World Economic Forum, *Global Risks Report 2025* (2025).